

# DECODIFICANDO

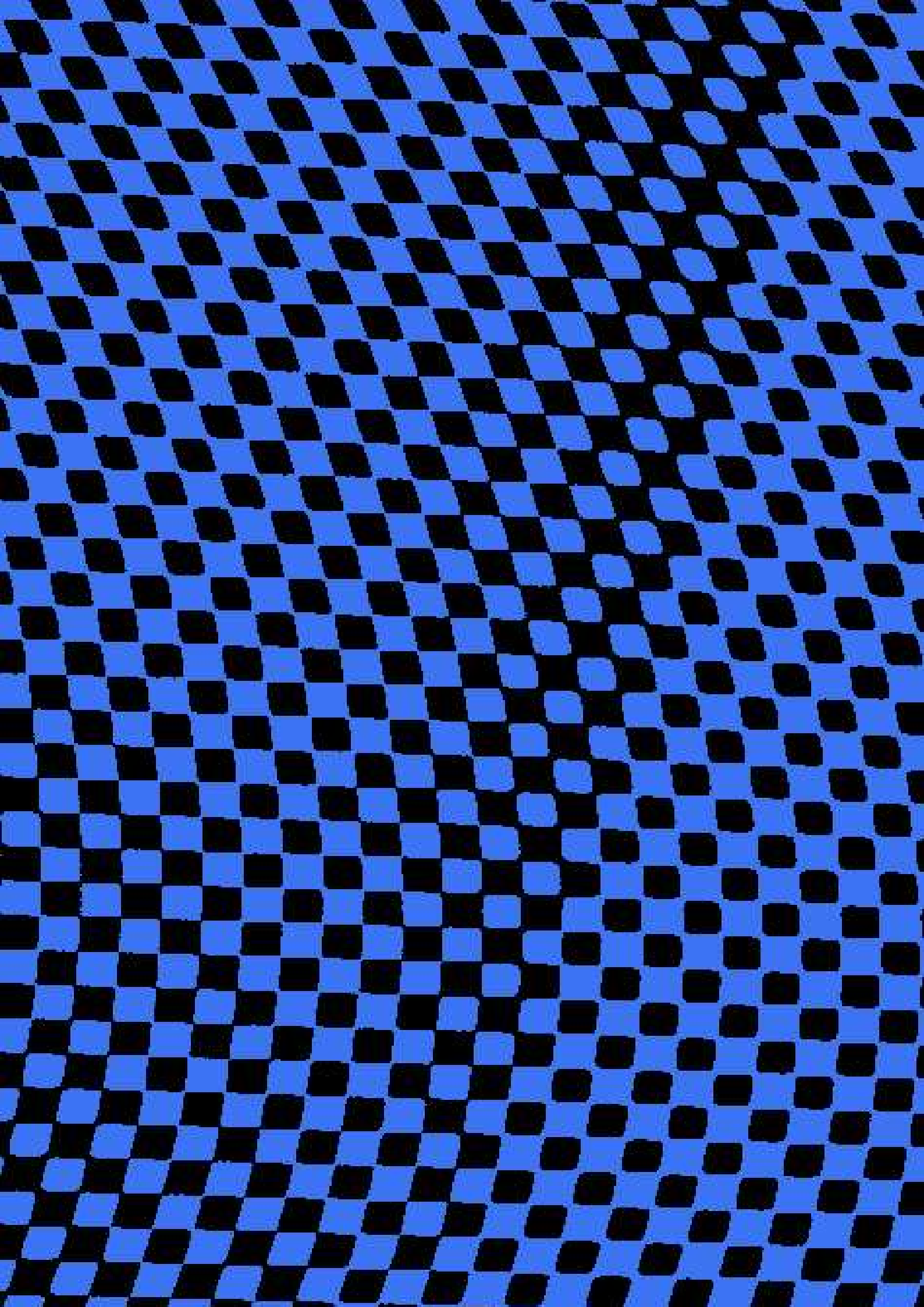


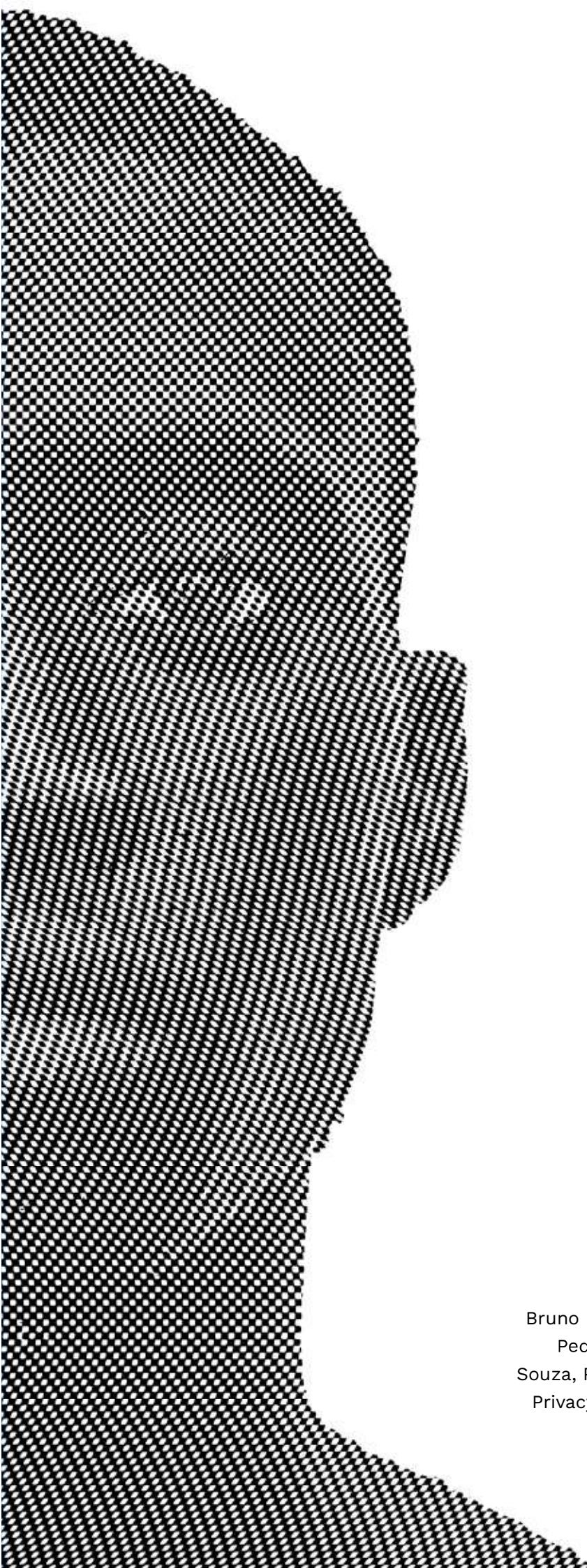
# LGPD

**X** DIÁLOGOS ENTRE A GERAÇÃO CIDADÃ DE  
DADOS, A LEI GERAL DE PROTEÇÃO DE DADOS  
E A JUSTIÇA RACIAL

# GCD







## **Agradecimentos**

Thiago Nascimento, Mariana de Paula

Bruno Bioni, Yuri Lima, Paulo Rená, Mariana Rielli,  
Pedro Martins, Vinicius Padrão, Carlos Affonso  
Souza, Paulo Rogério Nunes, Horrara Moreira, Data  
Privacy, Labid<sup>2</sup>, Data\_labe, Aqualtune Lab, Nic Br,  
CGI, Vale do Dendê, Rede GCD

## FICHA TÉCNICA

### Diretoria do Instituto Decodifica

Mariana de Paula  
Thiago Nascimento

### Coordenação Geral do Projeto

Bruno Sousa

### Coordenador Adjunto

Cláudio Mendes

### Edição

Pedro Paulo Silva

### Autores

Cláudio Mendes  
Johanna Monagreda  
Kayo Moura  
Luize Ribeiro  
Manuela Oliveira  
Pedro Saliba  
Polinho Mota

### Comunicação

Andy Pereira  
Cinthya Maldonado  
Max Chagas

### Capa e ilustrações

Andy Pereira

### Diagramação

Refinaria Design

### Dados Internacionais de Catalogação na Publicação (CIP)

Decodificando [livro eletrônico]: diálogos entre a geração cidadã de dados, a lei geral de proteção de dados e a justiça racial / Cláudio Mendes...[et al.] ; coordenação Bruno Sousa ; Ilustração Andy Pereira. — Rio de Janeiro : Labjaca, 2024.

Formato: PDF

ISBN: 978-65-985215-0-9

1. Tecnologia. 2. Geração cidadã de dados. 3. Lei geral de proteção de dados.  
4. Racismo. 5. Favelas. I. Mendes, Cláudio. II. Sousa, Bruno. III. Pereira, Andy. IV. Título.

CDD-341.27

Sueli Costa - Bibliotecária - CRB-8/5213 (SC Assessoria Editorial, SP, Brasil)

Índices para catálogo sistemático: 1. Direito :  
Lei geral de proteção de dados 341.27

# Manifesto

---

Decodificar: traduzir, compreender, converter, decifrar. Transformar o complexo em compreensível, o código em clareza. **É isso que o Instituto Decodifica faz.**

Sonhamos com um Brasil onde o CEP não define o futuro, onde a cor da pele não limita oportunidades. **Um Brasil onde cada voz importa, onde cada história é valorizada.**

Há quatro anos, nascemos na favela do Jacarezinho, em meio à pandemia. A crise da Covid-19 nos impulsionou a ir além, gerando dados, comunicando e mobilizando por soluções reais.

**Existimos para ajudar a preencher essa lacuna de dados que moldam políticas públicas, muitas vezes distantes da realidade e dos saberes das periferias.** Essa desconexão resulta em decisões ineficazes, recursos mal investidos e oportunidades perdidas para melhorar a vida nessas comunidades.

A nossa missão é **promover transformação social a partir do protagonismo dos saberes periféricos** e nos posicionar como **referência do Sul Global** na produção, articulação e coletivização de saberes a partir das periferias.

Isso se traduz em nossos estudos sobre **gênero, meio ambiente e clima, segurança pública e tecnologia** – pilares de nossa atuação –, sempre com a perspectiva de uma justiça racial que seja reparatória.

**Impulsionamos narrativas** de impacto, **realizamos formações** e fóruns locais, formando **novos quadros e lideranças**. Participamos ativamente de conferências nacionais e internacionais, disputando esses espaços para uma participação social mais ativa. Isso é uma pequena parte do que já fizemos coletivamente, e é só o começo.

Através da **geração cidadã de dados**, vamos coletivamente desvendar problemas e propor soluções, **nos conectando com favelas e periferias de todo o país. Juntos, imaginamos o futuro que queremos e partimos para construí-lo.**



Prefácio	8
Pedro Paulo Silva	
A proteção de dados pessoais no Brasil: um direito fundamental autônomo	10
Johanna Monagreda e Pedro Saliba	
Justiça Racial e Proteção de Dados: O Desafio do Colonialismo Digital	32
Manuela Oliveira e Luíze Pereira Ribeiro	
Aplicação da LGPD nas Instituições de Pesquisa que utilizam metodologia Geração Cidadã de Dados	60
Luíze Ribeiro e Manuela Oliveira	
A importância da Participação Cidadã para uma efetiva Cultura de Proteção de Dados	86
Kayo Moura e Cláudio Mendes	
Soberania de Dados	105
Polinho Mota	
Conclusão Desenhando o futuro: um marco para a GCD	118
Bruno Sousa	

# Prefácio

por Pedro Paulo Silva

Na era digital, os dados têm se revelado como as novas pedras preciosas e especiarias em nosso contexto histórico, conferindo valor inestimável à sociedade moderna. Desde ações cotidianas, como a compra de medicamentos, a entrada em eventos esportivos, ou a postagem em redes sociais, os dados coletados são transformados em inteligência. Essa inteligência é utilizada para uma ampla gama de propósitos, que vão desde decisões eleitorais e estratégias de marketing até o encarceramento e a justificativa de operações policiais.

No entanto, o valor intrínseco dos dados também expõe um risco significativo: sua extração e uso indevido podem resultar em consequências prejudiciais. Para mitigar esses riscos, foi implementada no ordenamento jurídico brasileiro a Lei Geral de Proteção de Dados (LGPD), que visa regulamentar a coleta, o processamento e o armazenamento de informações pessoais, garantindo que os direitos dos indivíduos sejam respeitados e protegidos. A LGPD representa um esforço crucial para equilibrar o uso das informações com a necessidade de proteger a privacidade e a segurança dos indivíduos.

Simultaneamente, os dados têm o potencial de ser um recurso valioso para o desenvolvimento de políticas públicas eficazes e direcionadas. A utilização de dados para formular políticas que atendam aos desejos e necessidades das populações mais vulneráveis pode promover

uma sociedade mais justa e equitativa. Nesse contexto, a metodologia de Geração Cidadã de Dados (GCD) surge como uma ferramenta inovadora. A GCD busca envolver diretamente os cidadãos na produção da pesquisa, possibilitando a produção de informações que refletem mais autenticamente as realidades e aspirações das comunidades, particularmente aquelas marginalizadas.

O Instituto Decodifica, por exemplo, adota uma versão da GCD com o objetivo de amplificar a voz e os interesses das populações negras e das comunidades periféricas, influenciando a formulação de políticas públicas que considerem suas necessidades e perspectivas.

Contudo, essa abordagem também levanta uma questão crucial: ao produzir e utilizar esses dados, não estamos, inadvertidamente, colocando em risco as próprias populações que pretendemos ajudar?

Este livro se propõe a abordar precisamente essa questão. Nosso objetivo é explorar como a proteção de dados deve ser manejada dentro das organizações envolvidas na Geração Cidadã de Dados, à luz da LGPD. Além disso, pretendemos investigar como essa discussão sobre privacidade e proteção de dados se entrelaça com questões de justiça racial. Reconhecemos que o debate sobre a legislação de proteção de dados tende a ser altamente técnico, o que pode afastar o público geral e obscurecer a relevância política dessas questões.

Portanto, este livro também visa trazer a política de volta ao centro da discussão, destacando como a proteção de dados e a justiça racial se interconectam e se influenciam mutuamente. Acreditamos que, ao tornar o debate mais acessível e relevante para todos, podemos promover uma abordagem mais inclusiva e equitativa na formulação e implementação de políticas públicas, garantindo que os dados, enquanto recurso precioso, sejam utilizados de maneira ética e justa.

No primeiro capítulo, temos Johanna Monagreda e Pedro Saliba, do Data Privacy, discutindo como a proteção de dados é um direito fundamental. Abandonando o debate europeu sobre proteção de dados como ponto de partida, Monagreda e Saliba escolhem o contexto Afro-Latino Americano, com destaque para a Constituição Brasileira, para demonstrar a importância do direito fundamental à privacidade em nosso ordenamento jurídico. E que, por isso, invasões de domicílios em operações policiais violam um direito fundamental ao invés de somente uma legislação de proteção de dados.

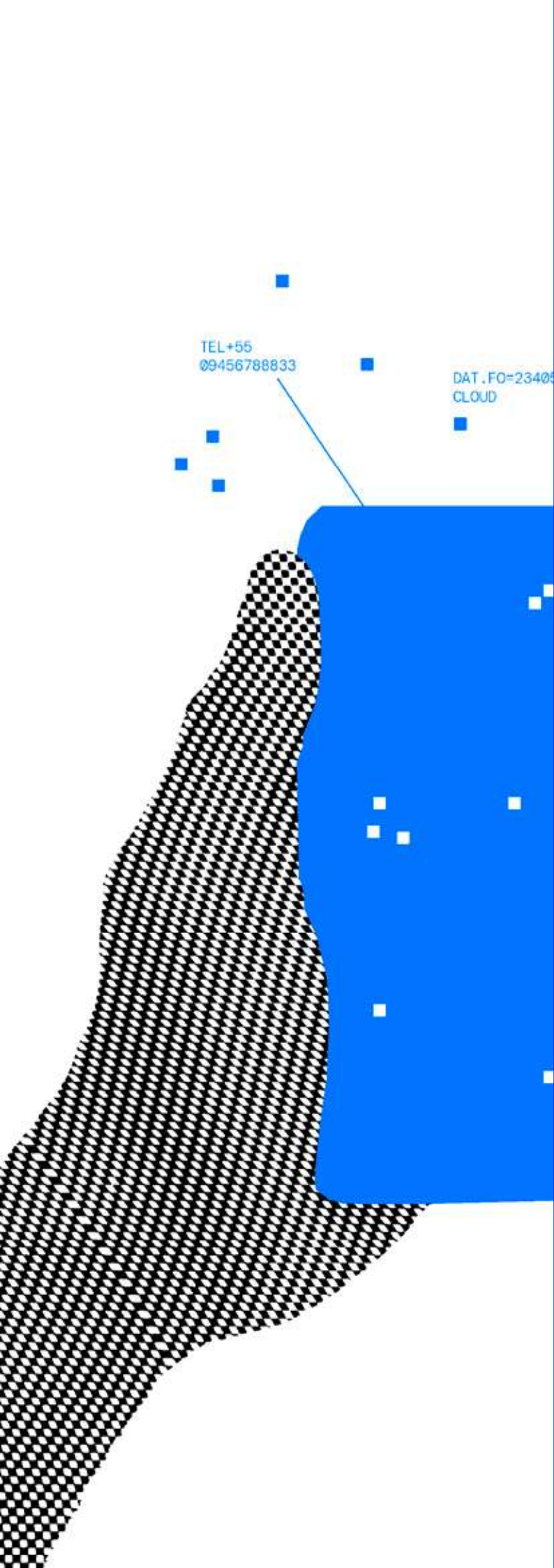
No segundo capítulo, Manuela Oliveira e Luíze Pereira Ribeiro, do Laboratório de Inovação e Direitos Digitais da Universidade Federal da Bahia (Labid<sup>2</sup>), nos contam sobre a interseção entre proteção de dados e justiça racial. O capítulo passa por conceitos fundamentais como reconhecimento facial, inteligência artificial (IA) e o racismo algorítmico, para tecer

uma análise sobre como o racismo perpassa essas tecnologias. Também colocam pontos de potencial resistência ao racismo dentro do campo de tecnologias e da proteção de dados.

No terceiro capítulo, também escrito por Oliveira e Ribeiro, as autoras destrincham a parte mais técnica da LGPD com objetivo de facilitar seu entendimento para o leitor não inteirado na discussão. Esse movimento é feito especificamente no que tange à GCD, de modo com que as organizações que utilizam essa metodologia possam gerar dados sem vulnerabilizar as populações negras e periféricas.

No quarto capítulo, Kayo Moura e Cláudio Mendes, do Instituto Decodifica, trazem o debate acerca da geração cidadã de dados. Os autores revisam esse conceito, sem objetificar dar uma única definição para o mesmo, mas trazendo a versão que o Instituto Decodifica utiliza. Em outro momento, se discute como gerar uma cultura de proteção de dados a partir do nosso contexto atual no Brasil.

Por último, Polinho Mota, do data\_labe, discute um conceito fundamental para toda essa discussão: o de soberania de dados. O autor a partir de uma perspectiva afro-brasileira, coloca que não temos soberania de dados, dentre outros motivos, por não possuímos controle sobre a infraestrutura de dados. Mas também coloca que existem iniciativas que trabalham para que consigamos a soberania de dados ou que tentam construir outras formas de soberania.



# A PROTEÇÃO DE DADOS PESSOAIS NO BRASIL: UM DIREITO FUNDAMENTAL AUTÔNOMO<sup>1</sup>

**Johanna Monagreda**

**Pedro Saliba**

*Data Privacy Brasil*

<sup>1</sup> A organização deste artigo deve muito às discussões sobre direitos dos titulares organizadas pela Data Privacy no marco do curso para a ANPD. Contudo, as ideias expostas são responsabilidade exclusiva dos autores.



### **JOHANNA MONAGREDA**

Doutora e Mestre em Ciência Política pela Universidade Federal de Minas Gerais. Fez Licenciatura em Ciência Política e Administrativa na Universidad Central de Venezuela. É pesquisadora do Núcleo de Estudos e Pesquisas sobre a Mulher NEPEM/UFGM, e autora da tese: “El Estado no nos ha regalado nada: Procesos de institucionalização das demandas dos movimentos afrodescendentes em Brasil, Venezuela e Equador”. Ao longo da sua trajetória profissional atuou em importantes pesquisas na área de direitos humanos, políticas de igualdade racial e políticas para mulheres na América Latina.

### **PEDRO SALIBA**

Advogado e sociólogo, mestre em Sociologia e Antropologia (PPGSA/UFRJ). Pesquisa sobre a intersecção entre proteção de dados pessoais e administração pública, especialmente questões de segurança e vigilância. Anteriormente atuou como pesquisador no Laboratório de Estudos Digitais (LED/UFRJ) e atualmente é coordenador de Assimetrias e Poder na Data Privacy Brasil.



# Introdução

**Preto tem que ter nome e sobrenome,  
senão os brancos arranjam um apelido... ao gosto deles.**

Lélia Gonzalez (1935-1994)

Ao abrir este diálogo com a intelectual brasileira Lélia Gonzalez nos interessa salientar a importância da identificação que cada pessoa faz de si própria, do seu território, da sua realidade; a forma em que a dignidade humana pode se ver afetada quando esse direito de auto-identificação é alienado, e; a relevância da possibilidade de decidir sobre as formas em que nos tornamos visíveis, representadas e tratadas em sociedade.

A socióloga norte-americana Patricia Hill Collins (2014), nos ensina que os distintos estereótipos e imagens de controle impostos pelo racismo e outras formas de opressão cumprem o papel de controlar e reduzir a existência das pessoas racializadas na subalternidade, bem como de delimitar as formas de visibilidade, representação e tratamento.

Este artigo tem como objetivo apresentar uma das ferramentas jurídicas atuais que permite que a cidadania exerça controle e participe das decisões sobre o tratamento das suas informações pessoais: o direito fundamental à proteção de dados pessoais.

Dados pessoais são todas aquelas informações que nos identificam ou nos tornam identificáveis. A partir dos nossos dados pessoais podemos ser identificadas, classificadas, avaliadas, representadas, bem como nossos territórios. Diversas decisões podem ser tomadas a partir de informações obtidas na análise desses dados.

Há interesse público e interesse comercial por trás da circulação dos nossos dados pessoais, uma vez que estes são fundamentais para o funcionamento da administração pública, para a execução de políticas públicas, para o monitoramento legítimo do Estado, para a oferta de produtos comerciais, etc. Entre outros usos, dados pessoais nutrem as tecnologias que funcionam com algoritmos, a internet, redes sociais, as câmeras de reconhecimento facial.

Mas para além desses propósitos instrumentais, é importante sempre lembrar que a proteção de dados pessoais é um direito fundamental autônomo vinculado à dignidade humana, o livre desenvolvimento da personalidade e a não-discriminação. Quer dizer, o que justifica a existência deste direito não é a necessidade de políticas públicas, nem a necessidade de estabelecer relações comerciais, mas a tutela da condição humana, inclusive no processo de formulação de políticas públicas e/ou nas práticas de mercado.



Assim, há uma diferença fundamental entre o direito à privacidade e o direito à proteção de dados pessoais, enquanto o primeiro se refere a possibilidade de resistir a intromissão do Estado e/ou do setor privado nas nossas vidas, a garantia do sigilo ou de ser deixado só, o direito à proteção de dados pessoais, estabelece garantias para que o titular possa ter controle sobre a circulação dos seus dados, e para o uso legítimo destes por parte do Estado ou do setor privado.

O capítulo está estruturado em 7 partes. Na primeira parte se discute o direito à proteção de dados pessoais como um direito fundamental, a segunda apresenta o titular de dados pessoais dentro de um contexto de desigualdades estruturais, a terceira seção descreve brevemente o percurso da regulamentação do direito à proteção de dados pessoais, na seção 4 se apresentam os princípios da Lei Geral de Proteção de Dados Pessoais, na quinta seção se introduz a discussão sobre os riscos do uso abusivo dos dados pessoais, nas seções 6 e 7, se tecem algumas considerações sobre a implementação da LGPD e as percepções da cidadania sobre o marco regulatório da proteção de dados pessoais no Brasil. Com isso, buscamos trazer subsídios não apenas ao debate, mas à atuação prática de organizações que utilizam dados pessoais em seus trabalhos. Ao compreender como sistemas informatizados podem afetar direitos e garantias, ativistas e pesquisadoras podem incidir com maior assertividade em políticas públicas e projetos.

## Direito fundamental à proteção de dados pessoais

---

O direito à proteção de dados pessoais reconhece a *potestad*<sup>1</sup> das pessoas de exercerem formas de controle sobre a circulação das suas informações pessoais, contra a discriminação, e em respeito à autonomia, a individualidade, a igualdade e a liberdade, elementos indispensáveis para o livre desenvolvimento da personalidade.

Apesar de muitas vezes se relacionarem, a proteção de dados é diferente da privacidade. O direito à vida privada diz respeito ao direito dos indivíduos de viverem suas próprias vidas, com suas particularidades e segredos em aspecto interior, relacionando-se diretamente com a intimidade (Silva, 2010, p. 103). A proteção de dados, por sua vez, versa sobre o fluxo de informações no mundo contemporâneo, entendendo ser necessária a circulação na sociedade. Em uma compra *online* é preciso saber o nome e endereço, assim como uma política de assistência social precisa de informações sobre renda e família para definir quem tem direito ao benefício.

---

<sup>1</sup> Poder, competência, faculdade.

No Brasil, a proteção de dados pessoais é considerada um direito fundamental reconhecido mediante a Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Conceitualmente, direitos fundamentais são direitos inerentes à condição humana reconhecidos na Constituição. Estabelecem a proteção da pessoa humana frente ao poder do Estado e a responsabilidade deste em garantir o mínimo necessário para uma existência digna. São universais, pois correspondem a todos os indivíduos; indivisíveis e interdependentes, já que o exercício de um depende da garantia do outro; e inalienáveis, ou seja, são inerentes à nossa existência.

Incluir a proteção de dados entre os direitos fundamentais, significa o reconhecimento da proteção de dados como um elemento essencial para garantir a afirmação da dignidade humana, uma vez que a vulneração do direito ou o uso abusivo dessas informações pode, potencialmente, ferir a igualdade e a dignidade da pessoa humana.

Ao adquirir *status* constitucional, pode-se entender que os princípios da proteção de dados pessoais devem ser atendidos em todas as situações, inclusive na inexistência de uma lei específica para determinado assunto e que todos os poderes públicos: executivo, legislativo e judicial têm obrigações na efetivação do direito.

Alguns autores têm questionado como a orientação liberal, individualista e universalista dos direitos fundamentais “impede a materialização do direito e cria obstáculos para a manutenção da eficácia das normas constitucionais em função da distância entre o discurso jurídico e a realidade social na qual as pessoas vivem” (Moreira 2016, 1560). A partir de uma análise sobre o contexto brasileiro, o jurista Adilson Moreira (2016) propõe uma compreensão dos direitos fundamentais como prerrogativas com caráter anti-hegemônico, com o potencial de “desestabilizar desigualdades de *status* e de desigualdades materiais” (Moreira 2016, 1565), onde o compromisso constitucional com o combate à marginalização, a busca pela igualdade efetiva e as políticas não-universalistas seriam elementos centrais para o exercício efetivo dos direitos fundamentais:

**Precisamos defender a posição que, junto com as funções mencionadas, os direitos fundamentais também devem ser vistos como estratégias anti-hegemônicas. Essa categoria de direitos precisa ser pensada como instrumentos que possibilitam a desconstrução de hierarquias entre grupos sociais, uma vez que as desigualdades são produto das relações assimétricas de poder entre grupos**

(Moreira 2016, 1584)

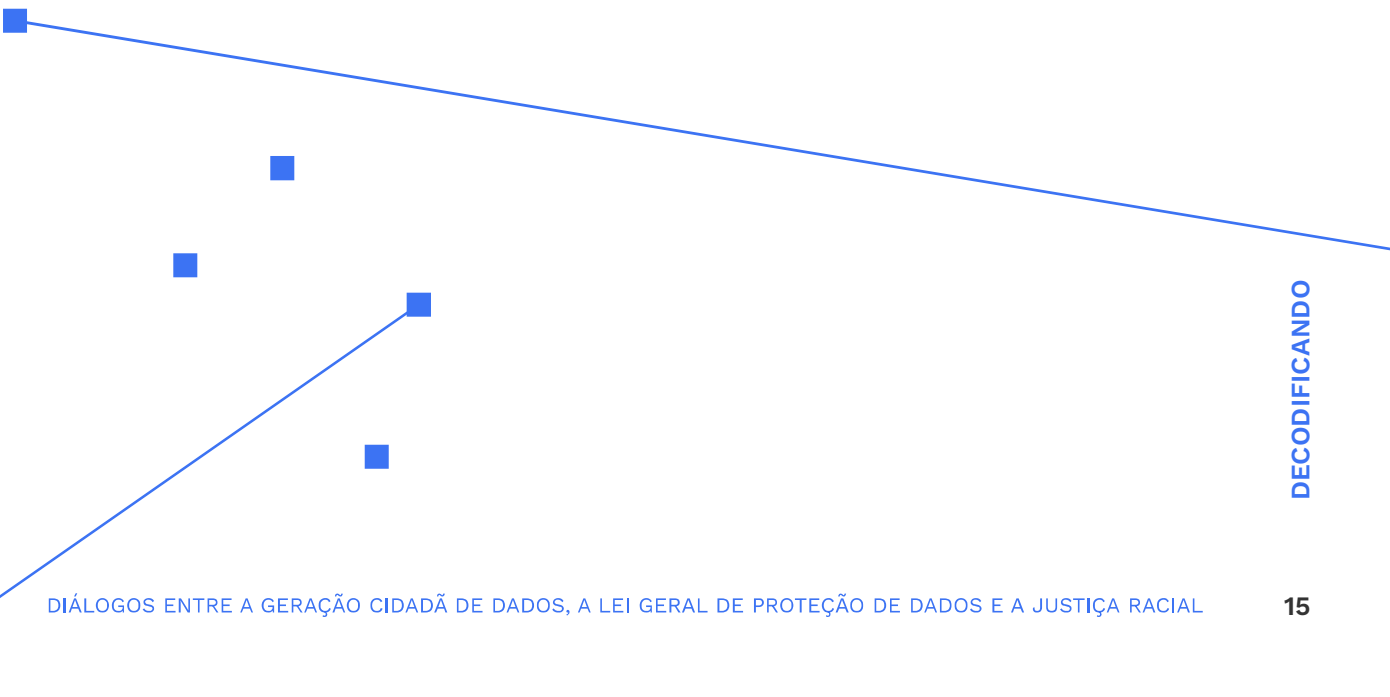


A perspectiva social de Moreira (2016) salienta a dimensão objetiva dos direitos fundamentais segundo a qual, estes são tanto as garantias individuais, quanto a ação estatal para a transformação social e a real efetivação do direito, inclusive por meio da ação diferenciada para grupos sociais. Esta perspectiva reconhece como as estruturas de poder produzem iniquidades que afetam a própria condição de sujeitos de direito para determinados grupos sociais, e outorga ao Estado um papel atuante na correção das desigualdades sociais.

E isto, não é diferente com relação à proteção de dados pessoais: A despeito das origens europeias dos direitos fundamentais e seu viés liberal-individualista, no Brasil a discussão sobre esses tipo de direitos precisa levar em consideração o fato de que as hierarquias e desigualdades estruturais representam barreiras reais ao gozo de direitos para diferentes grupos sociais (Moreira 2016). Sendo assim, “[o] dever de proteger pode envolver, por exemplo, o dever de interpretar a lei, tendo em conta a vulnerabilidade dos consumidores e a sua necessidade de proteção, ou o dever do Estado de desenvolver um sistema regulamentar para proteger os consumidores” (Doneda e Mendes 2014, 7).

Um dos momentos chave que contribuiu para o entendimento da proteção de dados como um direito fundamental autônomo no Brasil foi a ação contra a Medida Provisória (MP) 954/2020 que obrigava empresas de telefonia a compartilhar dados pessoais dos seus clientes com a Fundação do Instituto Brasileiro de Geografia e Estatística (IBGE) a fim de dar suporte a produção estatística do órgão no período da pandemia. A decisão do STF, para a qual a própria Data Privacy participou como *Amicus Curie* (Bioni, Zanatta, e Rielli 2021), suspendendo essa prerrogativa e argumentando a inconstitucionalidade da MP reforçou a relevância da proteção de dados pessoais, com um princípio importante para a tutela da dignidade humana e o livre desenvolvimento da personalidade, inclusive frente a uma finalidade pública legítima.

Como se verá na seguinte seção, o princípio da universalidade do direito à proteção de dados pessoais carrega em si o desafio de entender os entraves ao exercício igualitário do direito em contextos societários definidos por profundas desigualdades históricas que marcam os e as titulares dos dados.



## Quem é o titular de dados pessoais no Brasil: desigualdades estruturais e dignidade humana

O direito à proteção de dados pessoais tem como fundamento a pessoa humana. Contudo, as questões da dignidade da pessoa humana, do livre desenvolvimento da personalidade e da não-discriminação, que dão sustento ao direito fundamental, são constituídas por processos históricos de produção de desigualdades e marginalização.

A titularidade dos dados pessoais é uma ferramenta jurídica muito interessante, porque supõe uma continuidade entre a pessoa e o processo de datificação. Inclusive, dentro da dogmática jurídica, a proteção de dados tem como origem o direito de personalidade (Mendes, 2019), que protege aspectos fundamentais de seres humanos, como seu corpo, seu nome e privacidade. Esse nexo inquebrantável entre o corpo físico e sua expressão datificada permite representações e avaliações sobre os sujeitos com implicações concretas na vida das pessoas, justificando a proteção de dados como uma garantia sobre como os seres humanos são representados através dos dados.

No entanto, o *status* moral de pessoa, a condição humana que justifica o direito à proteção de dados está desigualmente distribuído, na prática, graças a processos históricos de construção dessa desigualdade. Se a expressão datificada do corpo deve ser protegida porque informa sobre a condição de pessoa humana, é relevante notar que para sujeitos que pertencem a grupos historicamente discriminados, a condição de pessoa foi sendo desconstruída a partir de processos concretos de dominação como a escravidão e a colonização que tem efeitos até hoje.

A soberania que é reconhecida ao titular sobre seus dados é importante desde um viés liberal-individualista para estabelecer barreiras à intervenção negativa do Estado e do mercado. Mas essa capacidade de estabelecer barreiras não está democraticamente distribuída na sociedade. As desigualdades estruturais, vieses raciais e socioeconômicos, na prática, limitam a possibilidade de reivindicar direitos (Kremer 2020). Como diversos autores têm salientado, as condições socioeconômicas são determinantes nos processos de mercantilização da cotidianidade e datificação da pobreza (Dencik et al. 2019; Martin e Taylor 2021; Masiero e Das 2019; Taylor 2017). Quanto mais distantes estão as pessoas do privilégio branco-masculino-heterossexual-de classe, fica mais evidente como a existência dessas barreiras e as opressões de raça, gênero e classe impactam nas decisões sobre tratamento de dados pessoais e limitam as possibilidades de proteção desses dados.

O filósofo político jamaicano Charles Mills (1997) nos auxiliará nesta análise. O autor argumenta que o racismo instaura uma partição ontológica do ser entre



pessoa (brancos) e sub-pessoa (que são os sujeitos da colonização) e isso tem implicações no próprio entendimento desse sujeito “subpessoa” como sujeito de direito, sujeito ao que corresponde a administração do poder, inclusive o poder de tomar decisões sobre o próprio corpo. Tem implicações nas formas em que o Estado entende suas obrigações com os diferentes grupos sociais; tem implicações na forma desigual em que o mercado respeita ou não os direitos dos seus consumidores; nas relações interpessoais que são mediadas por noções estereotipadas dos diferentes grupos sociais, e obviamente produz efeitos diferenciados sobre as pessoas e sobre os territórios.

Assim, a própria condição de titular dos seus dados pessoais se vê enfraquecida por essa construção ontológica que informa e limita a compreensão de sujeitos não-brancos e marginalizados em igualdade e como sujeitos de direito. De fato, é possível encontrar na legislação brasileira formas juridicamente estabelecidas de desconstrução da dignidade humana universal como a lei de vadiagem, que se refere aos artigos 14, 15 e 59 da Lei de Contravenções Penais (Lei nº 3.688/41), o argumento da Legítima defesa da honra, que só foi declarado inconstitucional em 2023, mas que era acionado para reduzir a pena em caso de feminicídio; e, o Estatuto do Índio de 1973 (Lei nº 6.001/73) que regulamenta a tutela dos indígenas através da FUNAI, imposição legal que estabelecia uma espécie de minoridade na população indígena, extinta em 1988 com a Constituição Cidadã.

A exposição desses exemplos não tem como objetivo discutir o embasamento jurídico da desigualdade, e sim pensar em como a internalização desses estereótipos sobre os grupos sociais podem estar acompanhando os processos de datificação. E como isso explica, tanto as práticas abusivas do mercado, quanto a dificuldade do titular de dados pessoais peticionar pelos seus direitos, por exemplo.

Aqui nos aproximamos do pensamento de Anita Allen (2022), Bianca Kremer (2020), Mariah Rafaela Silva (2020), Caitlin Mulholland (2018), Ramon Costa (2022), entre outros autores quando salientam a importância de entender o titular de dados de uma forma que leve em consideração a condição de raça, gênero, classe e sexualidade. Trata-se de um sujeito atravessado por marcadores de opressão, por construções sócio-históricas, por processos de hierarquização, marginalização e exploração, por produção de hegemonia e de intersubjetividades, de modo que não existiria um sujeito universal titular de dados, e a igualdade precisa ser posicionada como um princípio axiológico, um valor moral a ser alcançado.

Nesse sentido, a efetividade do direito à proteção de dados descansa ao mesmo tempo na reafirmação do valor axiomático do ideal de igualdade da pessoa humana, e do estabelecimento de instrumentos regulatórios e operativos que permitam desfazer essas barreiras, possibilitar um efetivo controle dos cidadãos sobre seus dados, e a garantir o papel do Estado no cumprimento do dever de proteção de dados pessoais através da regulação.

# A regulamentação do direito à proteção de dados no Brasil

Para traçar o caminho da regulamentação do direito à proteção de dados pessoais no Brasil até a Lei Geral de Proteção de Dados (LGPD) iremos dividir em três grupos de garantias a proteção de dados pessoais: a) garantias constitucionais, b) garantias nas relações de consumo e, c) garantias frente a burocracia estatal.

## *a. Garantias constitucionais: direitos fundamentais e habeas data*

### **Art. 5º: direitos e garantias fundamentais**

A Constituição Brasileira aborda diretamente questões relativas à informação ao prever os direitos fundamentais de liberdade de expressão (Art. 5º, IX; Art. 220) e acesso à informação e transparência (Art. 5º, XIV; Art. 220; Art. 5º, XXXIII; Art. 5º, XXXIV). Além disso, reconhece a inviolabilidade da vida privada e da privacidade (art. 5º, X) e também das comunicações telefônicas, telegráficas e de dados, (art. 5º, X, XII) e estabelece que o lar é o refúgio sagrado e inviolável do indivíduo. (Art. 5º, XII). Apesar de não dizerem respeito diretamente à proteção de dados pessoais, esses direitos são importantes para pensar o fluxo informacional, especialmente com tecnologias de informação e comunicação digitais.

A partir de 10 de fevereiro de 2022, a Emenda Constitucional nº 115 foi aprovada, reconhecendo oficialmente a proteção de dados pessoais no artigo 5º, LXXIX, da Constituição Federal. Antes disso, o Supremo Tribunal Federal (STF) já havia consagrado o direito à autodeterminação informativa<sup>2</sup>, sendo um marco importante porque demonstra como o tema é relevante para a cidadania contemporânea.

### ***Habeas data***

O *habeas data* é um instrumento constitucional que assegura acesso e retificação de informações pessoais que estejam em bancos de dados de entidades governamentais ou de caráter público. Previsto no artigo 5º, LXIX, ele foi incorporado na Constituição de 1988, sendo o Brasil o primeiro país do mundo a criá-lo.

<sup>2</sup> O direito foi reconhecido em 2020 nas Ações Diretas de Inconstitucionalidade (ADI) nºs 6.387, 6.388, 6.389, 6.390 e 6.393. O julgamento dizia respeito à possibilidade de compartilhamento de dados de empresas de telefonia para o Instituto Brasileiro de Geografia e Estatística (IBGE) para combate à pandemia com a Medida Provisória nº 954/2020. Esse compartilhamento foi considerado ilegal, tendo a proteção de dados como importante argumento nesse sentido.



A semelhança com *habeas corpus* não é à toa: enquanto um protege o corpo do abuso da ação estatal, contra prisões ilegais, por exemplo, o *habeas data* traz proteção semelhante para um bem intangível, os dados pessoais.

Concebido pelo jurista José Afonso da Silva, a inspiração veio das constituições da Espanha (1978) e de Portugal (1976), que previam a proteção de direitos frente ao avanço da informática, especialmente quanto ao uso de dados pessoais. No Brasil, havia uma preocupação bem evidente para a criação do *habeas data*: os abusos cometidos durante o Regime Militar brasileiro.

Segundo Sérgio Ribeiro (2013), trata-se de uma resposta da Constituinte à atuação invasiva do regime militar à privacidade de indivíduos mediante o Serviço Nacional de Informação (SNI) e outros órgãos públicos que, atuando em regimes de exceção, utilizam dados pessoais para perseguição política de opositores. O *habeas data* reconhece que o que se sabe sobre as pessoas pode afetar não apenas a privacidade, mas também outros direitos, como liberdade, integridade física e moral, convicções filosóficas.

Laura Mendes (2019) e Danilo Doneda (2017) reconhecem a aproximação entre *habeas data* e proteção de dados pessoais, sendo um instrumento jurídico que concretiza o direito à autodeterminação informativa, mesmo antes da LGPD entrar em vigor. Apesar dos avanços, Ribeiro (2013) aponta que há muitos obstáculos que impedem a utilização mais frequente do *habeas data*. Ainda assim, o protagonismo do Brasil inspirou outros países da América Latina a adotarem o instrumento em suas constituições, como Colômbia, 1991 (art. 15); Paraguai, 1992 (art. 135); e Peru, 1993 (art. 200, 3) (J. A. da Silva 2023, 171).

## *b. Garantias nas relações de consumo: Código de Defesa do Consumidor, Marco Civil da Internet e Lei de Cadastro Positivo*

### **Código de Defesa do Consumidor**

A proteção de dados, para além dos dispositivos constitucionais, emerge no Brasil como um tema de proteção ao consumidor. O Código de Defesa do Consumidor (CDC) traz de forma específica o direito a ser informado sobre coleta de dados, cadastros ou banco de dados e o direito do consumidor de acessar os dados que uma empresa tem sobre ele e pedir a correção desses dados. Em 2013 também o CDC é modificado para incorporar direitos à confidencialidade e segurança das informações pessoais prestadas ou coletadas.

Essas normas criaram um marco de interpretação para os tribunais. Através da regulação, consumidoras e consumidores contaram com uma proteção inédita sobre como são suas representações em dados, especialmente diante dos danos que pudessem ser causados.

## Lei de Cadastro Positivo

A Lei nº 12.414/2011 regula a formação e consulta a bancos de dados com informações de adimplemento para formação de histórico de crédito. Esse tipo de inferência, a respeito da capacidade de uma pessoa de honrar dívidas, pode afetar de formas distintas grandes parcelas da população, de modo que, dentre os direitos previstos, estão a indicação de gestores dos bancos de dados, acesso às informações constantes nos arquivos, indicação de quem consultou suas informações, entre outros. Em 2019, a Lei Complementar nº 166 atualizou a Lei de Cadastro Positivo com dispositivos que reforçam a proteção de dados pessoais, como transparência e política de utilização dos dados.

## Marco Civil da Internet

Em 2014, o Marco Civil da Internet (MCI) entrou em vigência como uma legislação para garantir direitos na rede. Tem princípios como a liberdade de expressão, a inviolabilidade da privacidade, neutralidade da rede e a própria proteção de dados pessoais (art. 3º, III, MCI). Foi essencial para o debate porque previa o direito de informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais (art. 7º, VIII, MCI), abrindo caminho para a promulgação posterior da Lei Geral de Proteção de Dados.

### *c. Frente à burocracia estatal: Lei de Acesso à Informação*

## Lei de Acesso à Informação

A Lei de Acesso à Informação (LAI) (Lei nº 12.527/2011) foi criada para regular o direito ao acesso à informação, previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal. Apesar de utilizar o termo “informação pessoal” (art. 4º, IV, LAI) e “tratamento da informação” (art. 4º, V, LAI), suas definições são próximas das dispostas pela LGPD, sendo um parâmetro importante para a disciplina no Brasil. Além disso, o direito de saber informações do Estado é essencial para o controle de políticas públicas. A LAI também prevê critérios como disponibilidade, autenticidade e integridade dos dados, essenciais para o fluxo adequado de informações. Destaca-se que, com a vigência da LGPD, houve muitos debates sobre a harmonia das duas legislações, com estudos demonstrando que houve negativa de acesso a informações utilizando de forma errônea a Lei Geral de Proteção de Dados como embasamento legal (Alves *et al.*, 2022).



# Lei Geral de Proteção de Dados Pessoais

A Lei Geral de Proteção de Dados (Lei nº 13.709/2018), também conhecida como LGPD, é o principal instrumento jurídico brasileiro para regular o tratamento de dados pessoais, garantindo nossos direitos como titulares dos dados. Fruto de mais de uma década de debates multissetoriais, sua aprovação demonstrou a importância de estabelecer regras para o tratamento de dados pessoais no Brasil, impedindo seu uso abusivo.

A lei é aplicável sobre dados de qualquer pessoa natural, ou seja, dados de empresas são regidos por ela. Tanto empresas quanto governos devem seguir suas regras quanto a dados digitais e físicos, se eles forem coletados ou tratados dentro do país. Poucas atividades são isentas de aplicação da LGPD, como jornalismo, trabalhos artísticos ou pesquisa científica. Outras, como atividades de segurança pública e inteligência, apesar de serem uma exceção de aplicabilidade da LGPD, ainda devem seguir seus princípios e direitos de titular.

Dentre seus fundamentos (artigo 2º, LGPD), além da privacidade, estão a autodeterminação informativa, liberdade de expressão, desenvolvimento econômico e tecnológico, direitos humanos, entre outros. Esses fundamentos demonstram o que a lei entende como um tratamento justo e lícito, devendo ser considerados em qualquer atividade que realiza tratamento de dados.

O artigo 18 da LGPD traz os direitos de titulares, ou seja, as garantias que cidadãs e cidadãos têm para que tenham um controle mínimo sobre suas informações. Alguns deles são o acesso aos dados, correção de dados incompletos, inexatos ou desatualizados, anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei, eliminação de dados e informações sobre o compartilhamento. Um desses direitos é a portabilidade dos dados: assim como você tem pode trocar de operadora de celular mantendo seu número, é possível pedir a portabilidade de seus dados para outro serviço ou produto.

Para zelar, implementar e fiscalizar o cumprimento da LGPD foi criada a Autoridade Nacional de Proteção de Dados (ANPD), responsável por estabelecer normas, protocolos e promover a cultura de proteção de dados no país. Além disso, qualquer pessoa pode peticionar à ANPD caso tenha seus direitos violados ou queira fazer uma denúncia.

## *d. Riscos do uso abusivo de dados pessoais*

Dados pessoais são fundamentais para auxiliar diversos processos de tomada de decisões. Para a formulação de políticas públicas, para a distribuição de recursos, para fins de marketing, ou inclusive para funcionamento de tecnologia

de inteligência artificial. Contudo, o uso abusivo de dados pessoais pode ter efeitos perversos na vida das pessoas, especialmente aquelas que pertencem aos grupos historicamente discriminados. Além da LGPD, todas as normas apresentadas são importantes para o combate a desigualdades e violações de direitos humanos que possam acontecer com dados pessoais. Abaixo traremos alguns exemplos nacionais e internacionais sobre esse tópico.

Dados pessoais podem ser usados para produzir tanto regimes de invisibilidade quanto de hipervisibilidade negativa ou discriminatória (Allen, 2022; Dencik et al. 2019; Martin e Taylor, 2021; Taylor, 2017), para perfilamento racial ou de gênero com efeitos de discriminação algorítmica e exclusão (Monagreda 2024; Noble 2018; O'Neil 2017; T. Silva 2022; Vilarino e Vicente 2020), com fins de desinformação, vigilância ilegítima (Allen 2022; G. Valente, Neris, e Fragoso 2021) ou inclusive tornar as pessoas mais vulneráveis a fraudes (Allen, 2022) colocando em risco os princípios de dignidade humana, livre desenvolvimento da personalidade e não-discriminação que são chave na procura pela tutela da condição humana.

As assimetrias de poder entre as empresas, os Estados, as corporações de tecnologia e, a cidadania titular dos dados colocam sérios entraves à efetivação do direito à proteção de dados pessoais. Fatores como falta de informação, carências materiais, situação de vulnerabilidade entre outros podem fazer com que as pessoas sejam pressionadas a abdicar do direito à proteção de dados pessoais quando outro direito está em jogo.

São diversos e cotidianos os casos em que a coleta de dados pessoais não parece responder aos parâmetros mínimos estabelecidos na legislação, o que torna imperativo o papel do órgão regulador. O problema de adequação à lei vai além de mecanismos formais, mas precisa da geração de uma cultura de proteção de dados pessoais, e da internalização de um senso de justiça que necessariamente chama a desconstruir as formas desiguais em que as pessoas são tratadas.

Um exemplo cotidiano, dessa relação desigual na direito à proteção de dados, são farmácias que oferecem descontos expressivos para pessoas com cadastros, podendo criar padrões de consumo na área da saúde extremamente valiosos para diversos setores da economia. A reportagem de Amanda Rossi (2023) no portal Uol, sobre o armazenamento abusivo e comercialização de dados pessoais, permite ter uma noção da dimensão do problema de coleta e armazenamento de dados pessoais pelas farmácias, traz também a dimensão da importância da comercialização de dados pessoais hoje, e nos permite pensar sobre uma espécie de privatização da proteção de dados pessoais, onde a garantia do direito parece estar mediado pelo poder aquisitivo. Quer dizer, que na prática, o direito à proteção de dados deixaria de ser universal, para se tornar um benefício de quem tem poder de compra o suficiente para, por exemplo, recusar um desconto quando informar dados pessoais se coloca como condição.

Essas desigualdades de poder para a efetivação do direito torna imperativo o papel dos órgãos de regulação. Em 2018, uma ação promocional da Unilever



com o Metrô do Rio de Janeiro coletava dados pessoais como nome, CPF e telefones em troca de um sachê de produto ultraprocessado<sup>3</sup>. Sem informações claras sobre o uso desses dados, as empresas foram notificadas pelo Instituto de Defesa de Consumidores (Idec) sobre a finalidade para coleta e preocupações com dados de crianças e adolescentes.

No Brasil, políticas de assistência social também apontam assimetrias informacionais do Estado com populações em situação de vulnerabilidade, especialmente quando o tratamento de dados pessoais é utilizado como forma de verificar fraudes. Valente, Neris, e Fragoso (2021) expõem violações à privacidade e controle social, tanto pelo Estado quanto por indivíduos, a beneficiárias do programa Bolsa Família, apontando como o desenho da cadeia de dados pessoais alimenta práticas difusas de vigilância, atingindo especialmente mulheres negras. Na Colômbia, López e Castro (2021) apontam questões similares, nas quais mulheres são expostas à crescente vigilância para verificação da condição de pobreza pelo Estado, demandando maior carga em comparação a outros membros da família.

A segurança pública é um dos setores onde uma cultura forte de proteção de dados poderia vir a contribuir com a garantia dos direitos humanos. Mesmo que a LGPD não seja aplicada em casos de segurança pública, a proteção de dados é um direito fundamental e os princípios deveriam ser aplicados. Mas diversas irregularidades sobre o uso desse recurso administrativo que são álbuns de suspeitos, é muito difícil exercer direito de acesso ou existência, é muito difícil inclusive obter resposta por LAI, e é muito difícil também exigir o direito de eliminação dos seus dados de álbuns de suspeitos. Essas práticas são opacas, sem controle sobre como as fotografias chegam às delegacias, tampouco se são excluídas, promovendo prisões de pessoas inocentes (Vergili *et al.*, 2022)

O Brasil tem desenvolvido algumas pesquisas que mostram que pessoas negras são alvos preferenciais do encarceramento por monitoramento facial, com índices de 90% de presos e presas negras no Rio de Janeiro (Nunes, Silva, e Oliveira 2022) (90%), que são as principais vítimas de reconhecimento errôneo pelo reconhecimento fotográfico (Vergili *et al.*, 2022). Tudo isso, alimentado em pressupostos racista, sexistas, etc., que alimentam as decisões sobre dados. Monitoramento e vigilância sobre pessoas negras, aumenta as chances de coleta de dados para criminalização.

Por fim, dois casos ilustram decisões que protegem cidadãos e cidadãs que utilizam aplicativos e redes sociais no Brasil. Apesar de ter muitos usuários e usuárias brasileiras, o Telegram e Signal, aplicativos de troca de mensagens, não tinham políticas de privacidade em português, prejudicando a compreensão pelo público brasileiro. Em 2022 a Defensoria Pública do Estado do Rio

---

<sup>3</sup> INSTITUTO DE DEFESA DE CONSUMIDORES. Idec notifica MetrôRio e Unilever por publicidade de ultraprocessados e uso de dados. 177 dez. 2018. Disponível em: <https://idec.org.br/noticia/idec-notifica-metrorio-e-unilever-por-publicidade-de-ultraprocessados-e-uso-de-dados>. Acesso em: 3 ago. 2024.

de Janeiro ingressou com uma Ação Civil Pública requerendo o cumprimento da lei, tendo uma decisão favorável nesse sentido (DPERJ, 2022). Em 2024, a ANPD proibiu que a Meta, empresa responsável pelo Facebook, Instagram e WhatsApp, utilizasse dados pessoais para o treinamento de inteligência artificial. A decisão se baseou na LGPD e apontou indícios de tratamento de dados pessoais com base em hipótese legal inadequada, além de falta de transparência, limitação aos direitos dos titulares e riscos para crianças e adolescentes (ANPD, 2024).

## Implementação da LGPD no Brasil

Nesta seção iremos apontar algumas das características da implementação da LGPD no Brasil. Para isso, consideramos duas pesquisas recentes que versam sobre a temática. A primeira é a pesquisa realizada pela Opice Blum em 2022, cujos resultados foram apresentados no Relatório anual de jurimetria (2022) e, a Pesquisa Painel LGPD nos Tribunais (2023) desenvolvida desde 2021 pelo Centro de Direito, Internet e Sociedade (CEDIS-IDP) do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP) e o Jusbrasil.

Resultados da *Pesquisa Painel LGPD* (2023) mostram que a LGPD está sendo aplicada cada vez com maior frequência pelo poder judiciário. Segundo a pesquisa, em 2021, a LGPD foi citada em 274 decisões de maneira relevante, esse número passou para 665 em 2022, e 1206 em 2023, mostrando-se um aumento expressivo na utilização da lei nos tribunais de justiça.

Esse dado é muito importante para pensar como a proteção de dados no Brasil está incrementalmente permeando a sociedade brasileira e seu sistema jurídico, de certa forma mostra como a própria existência da lei tem o papel de dar realidade ao direito, e a possibilidade de, de fato, se vir a consolidar uma cultura de proteção de dados no país.

Essas pesquisas sobre judicialização a partir da LGPD mostram que o direito a proteção de dados pessoais é também entendido como um instrumento para garantir outros direitos, por exemplo, pedidos de acesso e existência sendo ativados para buscar informações sobre seus dados que permitam fortalecer as ações trabalhistas, ou associadas aos direitos dos trabalhadores, e a LGPD é geralmente ativada quando se identifica um dano material ou moral.

O Relatório anual de jurimetria da Opice Blum (2022) ao indagar sobre as motivações das decisões que envolveram a LGPD encontrou que maior parte destas foram motivadas por situações envolvendo cobrança ou proteção ao crédito (45%), compartilhamento e divulgação (28%), Incidentes de Segurança (11%) como vazamento, e situações incluindo ações criminais, como fraudes bancárias e golpes (4%), entre outras.

A pesquisa da Opice Blum resulta interessante também para tecer algumas considerações sobre o papel do judiciário na interpretação da LGPD. Na maioria



dos casos, o incumprimento do princípio de transparência por parte do agente de tratamento dos dados é entendido como uma falta que leva à condenação, inclusive frente a existência de uma base legal que dispense o consentimento do titular, a transparência continua sendo considerado um princípio fundamental para atender o dever de justificar a atividade que realiza, adotar medidas de contenção de danos e, sobretudo, colocar-se sob escrutínio público, em observância ao princípio da prestação de contas.

Outro aspecto interessante da implementação da LGPD, identificado pela pesquisa da Opice Blum (2022) é que a maioria dos processos judiciais envolvendo a LGPD não resultaram em condenação (57%), determinando-se improcedentes. Entre as decisões com condenação, foi identificada, na pesquisa, uma quantidade maior de condenações envolvendo indenização, e menos envolvendo obrigações de fazer ou não fazer. Isto é interessante, porque a vocação da lgpd é justamente evitar a ocorrência de um dano, mas isto mostra que há uma tendência maior a utilizar a legislação para reparar danos morais ou materiais.

A comprovação de dano efetivo parece ser um critério para decisões favoráveis ao titular dos dados indicando tendência de que ele não possui natureza *in re ipsa* (presumido) no entendimento do poder judiciário, como reforçado na decisão do Superior Tribunal de Justiça (STJ) que, em 2023: “Ao vincular a possibilidade de reparação apenas ao vazamento de dados sensíveis ou íntimos, o julgado parece ter desconsiderado o paradigma da proteção de dados inaugurado com a LGPD, segundo o qual não existe dado pessoal insignificante, merecendo proteção qualquer dado pessoal, seja ou não sensível” (Laura Schertel Mendes em entrevista).

Condenações relacionadas a obrigações de fazer ou não fazer também figuram de forma cumulativa às condenações pecuniárias, representando a intenção do Judiciário tanto de remediar quanto de reparar violações aos direitos dos titulares, abrangendo cerca de 39% das decisões estudadas. Nos casos de obrigação de fazer, o direito à exclusão (art. 18) é o mais demandado nas decisões sobre os direitos dos titulares (67%).

Ainda, as pesquisas revelaram uma tendência a pedidos de informações sobre critérios e procedimentos utilizados em decisões automatizadas, que é um direito contemplado no artigo 20 da LGPD. O que mostra uma certa preocupação da cidadania sobre seus dados, em um contexto de uso incremental de aplicativos, redes sociais, sites de compras, etc.

É possível esperar um maior uso da LGPD na defesa de direitos e um maior apelo da sociedade brasileira pela proteção dos seus dados pessoais, na medida em que a discussão se democratiza. Em 2022 foi lançada uma pesquisa do Núcleo de Informação e Coordenação do Ponto BR que apresenta dados interessantes sobre a percepção da cidadania sobre seus dados pessoais, na seguinte seção apresentamos alguns desses resultados.

## Percepção da sociedade sobre a proteção de dados

Em 2022, o Núcleo de Informação e Coordenação do Ponto BR organizou a pesquisa Privacidade e proteção de dados pessoais: *perspectivas de indivíduos, empresas e organizações públicas no Brasil, 2021*. A um ano de funcionamento da Autoridade Nacional de Proteção de Dados (ANPD), a pesquisa traz informações relevantes sobre a adoção e conformidade com a LGPD por empresas e organizações públicas brasileiras, assim como da percepção da cidadania sobre a implementação da LGPD.

Os resultados permitem tecer algumas elucidações interessantes. Segundo a pesquisa, a maioria dos usuários da internet expressa preocupações sobre o tratamento dos seus dados pessoais e já tomou alguma medida na tentativa de exercer seu direito à autodeterminação informativa: 77% dos usuários de internet desinstalaram algum aplicativo do celular, 69% deixaram de visitar alguma página, 57% deixaram de utilizar algum serviço ou plataforma na internet e 45% dos usuários de Internet deixaram de comprar um aparelho eletrônico por causa de preocupações com seus dados. A prática de gerenciamento de acesso a seus dados pessoais mais utilizada em 2021 foi verificar a segurança de uma página ou aplicativo, por exemplo, se a página tinha cadeado de segurança (70%), enquanto a prática menos utilizada foi solicitar a páginas, aplicativos ou buscadores que apagassem informações sobre a si (42%).

Comparando com as distintas atividades realizadas na internet, os usuários expressaram um nível de preocupação maior com seus dados pessoais ao comprar pela Internet por páginas ou aplicativos (42%), e ao acessar páginas e aplicativos de bancos (35%), e um nível de preocupação muito menor ou nada preocupados ao enviar ou receber mensagens (28%), e ao usar plataformas de videoconferência e videochamadas (23%) e ao armazenar arquivos em nuvem (20%).

Os usuários de Internet se declararam muito preocupados com o fornecimento de informações pessoais sensíveis como biometria facial, impressão digital ou fotografia do rosto (41%) e dados de saúde (29%), e nada preocupados com o fornecimento de informações relativas à cor ou raça (44%), orientação sexual (43%) e crença religiosa (43%).



Os dados também mostram uma diferença no nível de preocupação sobre o uso dos dados feito pelas empresas no que tange à cor ou à raça do respondente. Pessoas pretas (52%) e pardas (49%) declaram estar muito preocupadas numa proporção maior do que brancas (43%), o que sugere uma percepção de potencial uso discriminatório desse dado por parte de empresas contra essa população. A diferença também ocorre quando o uso é feito por governos: 47% dos pretos declaram estar muito preocupados, enquanto esse percentual é inferior entre pardos (41%) e brancos (37%)

(Oyadomari, Costa, e Ribeiro 2023, 5)

Com relação à adequação das empresas a LGPD, a medida mais tomada foi o desenvolvimento de uma política de privacidade, contudo o número de empresas aderindo a essa medida foi baixo, 32%. Outras medidas nomeadas pelas empresas pesquisadas foram realização de testes de segurança contra vazamento de dados (30%), elaboração de um plano de conformidade ou adequação à proteção de dados pessoais (24%) e elaboração de relatório de impacto (13%).

A busca por canais de atendimento para solicitações, reclamações ou denúncias foi feita por 24% dos usuários de Internet com 16 anos ou mais. Entre os que buscaram, o canal mais mencionado foi a própria empresa ou órgão público controlador do dado (80%), seguido de órgãos de defesa do consumidor, como o Procon (48%). Já a ANPD aparece em um patamar bastante inferior (27%)

(Oyadomari, Costa, e Ribeiro 2023, 4)

Os dados revelam ainda que o órgão regulador da proteção de dados pessoais, a ANPD, não é percebido como a principal instância para reclamações ou resolução de problemas associados à vulneração desse direito. Sendo as instâncias de defesa ao consumidor mais frequentemente ativadas, o que provavelmente guarda relação com a longevidade do próprio CDC e sua incidência nos casos envolvendo relações clientes-empresas.

Ainda assim, é importante destacar que a LGPD foi aprovada em 2018, com vigência a partir de 2020. O próprio direito do consumidor, hoje bem conhecido pelas pessoas, teve uma intensa mobilização social e midiática para ter a difusão que tem hoje. Os próximos anos dirão como a proteção de dados tem sido apropriada pelo poder público, empresas e por cidadãos e cidadãs, cabendo novas pesquisas para acompanhar esse cenário.

## Considerações finais

---

Buscamos neste texto apresentar um cenário amplo sobre a proteção de dados pessoais e riscos a direitos fundamentais. Analisando o tratamento de dados em uma perspectiva que inclui raça, gênero, classe e sexualidade, apontamos a importância desses marcadores em uma defesa da dignidade da pessoa humana diante da sociedade contemporânea, muito pautada em sistemas digitais de datificação e classificação. No Brasil, uma série de legislações prevêem direitos e garantias nessa esfera, sendo a Lei Geral de Proteção de Dados a mais importante delas. Os exemplos sobre violações utilizando o tratamento de dados apontam um panorama prático das desigualdades causadas por novas tecnologias e um chamado à ação de ativistas e pesquisadoras em defesa dos direitos humanos.

Assim como a ausência de informações produz padrões de invisibilidade e exclusões, que podem ser reparadas mediante a Geração Cidadã de Dados, é importante lembrar que a proteção de dados pessoais pode ser uma ferramenta importantíssima para evitar que o tratamento desses dados se reverta em resultados perversos para a cidadania, em termos de discriminação, exclusão ou tratamento ilegítimo, especialmente entre os grupos historicamente vulnerabilizados e seus territórios.

Este artigo tem como objetivo apresentar uma das ferramentas jurídicas atuais que permite que a cidadania exerça controle e participe das decisões sobre o tratamento das suas informações pessoais: o direito fundamental à proteção de dados pessoais.

Em conjunto com os artigos da presente obra, esperamos contribuir para que indivíduos e organizações que se identifiquem com a Geração Cidadã de Dados estejam cientes dos potenciais e responsabilidades ao coletar e tratar dados pessoais, monitorando e denunciando irregularidades.

## Referências

Alves, C.; Brembatti, K.; Santos, J.; Ramalho, W. **Impactos da LGPD nos pedidos de LAI ao governo federal**. Disponível em: <https://fiquemsabendo.com.br/transparencia/relatorio-lai-lgp/>.

Autoridade Nacional de Proteção de Dados. ANPD determina suspensão cautelar do tratamento de dados pessoais para treinamento da IA da Meta. 2 jul. 2024. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-determina-suspensao-cautelar-do-tratamento-de-dados-pessoais-para-treinamento-da-ia-da-meta>. Acesso em: 20 ago. 2024.

Castro, N.. ‘Fotos que condenam’: homem ficou 10 meses preso injustamente e foi tido como criminoso 9 vezes por erro de reconhecimento. **G1**. 30 set. 2021. Disponível em: <https://g1.globo.com/rj/rio-de-janeiro/noticia/2021/09/30/fotos-que-condenam-homem-ficou-10-meses-preso-injustamente-e-foi-tido-como-criminoso-9-vezes-por-erro-de-reconhecimento.ghml>.

MENDES, L. S. F. Habeas data e autodeterminação informativa: os dois lados de uma mesma moeda. **Revista Brasileira de Direitos Fundamentais & Justiça**, [S. l.], v. 12, n. 39, p. 185–216, 2019. DOI: 10.30899/dfj.v12i39.655. Disponível em: <https://dfj.emnuvens.com.br/dfj/article/view/655>.

RIBEIRO, S. L. A.. **Habeas data e tutela jurisdicional da privacidade**: aspectos processuais. 2013. Dissertação (Mestrado em Direito das Relações Sociais) - Faculdade de Direito, Pontifícia Universidade Católica de São Paulo, São Paulo, 2013. Disponível em: <https://repositorio.pucsp.br/jspui/handle/handle/6222>.

Vergili, G.; Saliba, P.; Zanatta, R. **Injustiças procedimentais: repensando a relação entre dados pessoais e reconhecimento fotográfico**. In: Coletânea reflexões sobre o reconhecimento de pessoas: caminhos para o aprimoramento do sistema de justiça criminal. Conselho Nacional de Justiça; Coordenação Rogério Schietti Cruz, Mauro Pereira Martins, Luís Geraldo Sant’Ana Lanfredi – Brasília: CNJ, 2022. Disponível em: <https://www.cnj.jus.br/wp-content/uploads/2022/12/coletanea-reconhecimento-de-pessoas-v6-2022-12-06.pdf>. Acesso em: 3 ago. 2024.

Allen, Anita L. 2022. “Dismantling the ‘Black Opticon’: Privacy, Race Equity, and Online Data-Protection Reform”. *SSRN Electronic Journal*. doi:10.2139/ssrn.4022653.

Bioni, Bruno, Rafael Zanatta, e Mariana Rielli. 2021. “Caso: IBGE vs. CFOA B e outros (ADIs 6.387, 6.388, 6.389, 6.390 e 6.393) (Parecer).” *Revista de Direito Civil Contemporâneo* 26. <https://ojs.direitocivilcontemporaneo.com/index.php/rdcc/article/view/889>.

Costa, Ramon Silva. 2022. “Proteção de dados sensíveis de pessoas LGBTI+: perspectivas sobre personalidade, vulnerabilidade e não discriminação”. Em *Vulnerabilidades E Suas Dimensões Jurídicas*, org. Fabiana Rodrigues Barletta. Indaiatuba, SP: Editora Foco.

Dencik, Lina, Arne Hintz, Joanna Redden, e Emiliano Treré. 2019. “Exploring Data Justice: Conceptions, Applications and Directions”. *Information, Communication & Society* 22(7): 873–81. doi:10.1080/1369118X.2019.1606268.

Doneda, Danilo. 2017. “Iguais mas Separados: O Habeas Data no Ordenamento Brasileiro e a Proteção de Dados Pessoais”. *Cadernos da Escola de Direito* 2(9). <https://portaldeperiodicos.unibrasil.com.br/index.php/cadernosdireito/article/view/2607> (21 de agosto de 2024).

Doneda, Danilo, e Laura Schertel Mendes. 2014. “Data Protection in Brazil: New Developments and Current Challenges”. Em *Reloading Data Protection*, orgs. Serge Gutwirth, Ronald Leenes, e Paul De Hert. Dordrecht: Springer Netherlands, 3–20. doi:10.1007/978-94-007-7540-4\_1.

G. Valente, Mariana, Natália Neris, e Nathalie Fragoso. 2021. “Presença na rede de proteção social: privacidade, gênero e justiça de dados no Programa Bolsa Família”. *Novos Estudos - CEBRAP* 40(1): 11–31. doi:10.25091/s01013300202100010001.

Hill Collins, Patricia. 2014. *Black Feminist Thought: Knowledge, Consciousness, and the Politics of Empowerment*.

Kremer, Bianca. 2020. “LGPD em vigor: por que racializar a proteção de dados é tão importante?” *Jota Info. Opinião e Análise. Privacidade*. <https://www.jota.info/opiniao-e-analise/artigos/lgpd-em-vigor-protacao-dados-importante-01102020>.

López, Joan, e Laura Castro. 2021. “Vigilando a las ‘buenas madres’: Aportes desde una perspectiva feminista para la investigación sobre la datificación y la vigilancia en la política social desde Familias En Acción”. doi:10.13140/RG.2.2.10117.27368.

Martin, Aaron, e Linnet Taylor. 2021. “Exclusion and Inclusion in Identification: Regulation, Displacement and Data Justice”. *Information Technology for Development* 27(1): 50–66. doi:10.1080/02681102.2020.1811943.

Masiero, Silvia, e Soumyo Das. 2019. “Datafying Anti-Poverty Programmes: Implications for Data Justice”. *Information, Communication & Society* 22(7): 916–33. doi:10.1080/1369118X.2019.1575448.

Mills, Charles W. 1997. *The Racial Contract*. Ithaca: Cornell University Press.

Monagreda, Johanna Katiushka. 2024. “Por que falar de raça quando falamos de dados pessoais, inteligência artificial e algoritmos?” Em *Inteligência artificial e algoritmos - Desafios e oportunidades para os media*, orgs. Adriana Gonçalves, Luisa Torre, e Paulo Victor Melo.

Moreira, Adilson José. 2016. “Direitos Fundamentais como Estratégias Anti-Hegemônicas: Um Estudo Sobre a Multidimensionalidade de Opressões”. *REVISTA QUAESTIO IURIS* 9(3). doi:10.12957/rqi.2016.20235.

Mulholland, Caitlin Sampaio. 2018. “Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18)”. *Revista de Direitos e Garantias Fundamentais* 19(3): 159–80. doi:10.18759/rdgf.v19i3.1603.

Noble, Safiya Umoja. 2018. *Algorithms of oppression: how search engines reinforce racism*. New York: New York University Press.



Núcleo de Informação e Coordenação do Ponto br. 2022. *Privacidade e proteção de dados pessoais: perspectivas de indivíduos, empresas e organizações públicas no Brasil*. org. Comitê Gestor da Internet no Brasil. São Paulo, SP: Núcleo de Informação e Coordenação do Ponto BR.

Nunes, Pablo, Mariah Rafaela Silva, e Samuel R. de Oliveira. 2022. *Um Rio de olhos seletivos: uso de reconhecimento facial pela polícia fluminense*. Rio de Janeiro, RJ: CESec.

O'Neil, Cathy. 2017. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. First paperback edition. New York: B/D/W/Y Broadway Books.

Oyadomari, Winston, Ramon Silva Costa, e Manuella Maia Ribeiro. 2023. "Perspectivas da sociedade brasileira em relação à privacidade e à proteção de dados pessoais". *Panorama Setorial da Internet* 2(15).

Rossi, Amanda. 2023. "O que a farmácia sabe sobre mim". UOL. <https://noticias.uol.com.br/reportagens-especiais/o-que-a-farmacia-sabe-sobre-mim/>.

Silva, José Afonso da. 2023. *Comentário Contextual à Constituição*. 10ª ed São Paulo, SP: Editora Juspodivm.

Silva, Mariah Rafaela. 2020. "Código da ameaça: trans; classe de risco: preta". *São Paulo: N-1 Edições*.

Silva, Tarcízio. 2022. *Racismo algorítmico: inteligência artificial e discriminação nas redes digitais*. Edições Sesc SP.

Taylor, Linnet. 2017. "What Is Data Justice? The Case for Connecting Digital Rights and Freedoms Globally". *Big Data & Society* 4(2): 205395171773633. doi:10.1177/2053951717736335.

Vilarino, Ramon, e Renato Vicente. 2020. "An experiment on the mechanisms of racial bias in ML-based credit scoring in Brazil". doi:10.48550/ARXIV.2011.09865.

# JUSTIÇA RACIAL E PROTEÇÃO DE DADOS: O DESAFIO DO COLONIALISMO DIGITAL

Manuela Oliveira

Luize Pereira Ribeiro

RPFBR\_BCBR  
REAL\_VL

PAP\_TINT\_FIDUCI  
Y6,5  
X14 2

SLMINI\_  
1412/2024

AA002679123

## MANUELA OLIVEIRA

Compliance Officer e DPO em empresa de tecnologia, com especialização em Direito Digital, Gestão da Inovação e Propriedade Intelectual pela PUC Minas, além de graduação em Direito pela UFBA. Certificada em Compliance Anticorrupção pela LEC e DPO pela EXIN. Co-fundadora e conselheira no Laboratório de Inovação e Direitos Digitais (LABIDD) e pesquisadora no Legal Grounds Institute. Membro no Compliance Women Committee. Atuação em Justiça Social e Racial, Inteligência Artificial, Direito Registral e Proteção de Dados.

## LUIZE RIBEIRO

Pesquisadora bolsista do CNPq e convidada pelo Instituto Decodifica. Analista de Qualidade de Dados Jurídicos em empresa de tecnologia. Bacharela em Humanidades, com habilitação em Estudos Jurídicos pela Universidade Federal da Bahia (UFBA). Atualmente é estudante de Direito na mesma instituição. Membro do Laboratório de Inovação e Direitos Digitais da UFBA. Egressa da 15a South School on Internet Governance e Escola de Governança da Internet (EGI). Jovem liderança na Governança da Internet pelo Programa Youth Brasil de 2023 e 2024.

## Introdução

Em novembro de 2022, durante a festa de junina no Parque de Exposições, na cidade de Salvador, Bahia, um homem negro ficou preso injustamente, por 26 dias, por meio do uso de sistema de reconhecimento facial<sup>4</sup>. De forma semelhante, em abril de 2023, na cidade de Niterói, no Rio de Janeiro, um jovem negro foi preso injustamente e indiciado pela terceira vez por erro de identificação em reconhecimento facial<sup>5</sup>.

A tecnologia de reconhecimento facial, a qual utiliza inteligência artificial (IA), compreende na detecção da identidade de indivíduos “por meio de uma análise avançada de seus detalhes faciais” combinados com um banco de imagens de rostos e padrões visuais. Dessa forma, o processo de reconhecimento automatizado pode ser dividido em três etapas, sendo elas: reconhecimento do rosto; captura; e comparação de rosto com banco de imagens pré-existentes<sup>6</sup>.

Convém ressaltar que o reconhecimento facial por meio de IA é diferente do reconhecimento facial tradicionalmente conhecido em delegacias. No primeiro, o reconhecimento é automatizado, conforme já elucidado; enquanto no segundo, este reconhecimento decorre diretamente da memória humana, ou seja, por meio da comparação entre a memória da vítima e/ou testemunha com a apresentação de imagens – seja pessoalmente ou por meio de uma galeria de fotos – de suspeitos envolvidos em crimes.

Em 2014, o Governo de Goiás começou a utilizar essa tecnologia de forma pioneira no Brasil, por meio da instalação de câmeras de videovigilância em espaços públicos<sup>7</sup>. Em 2019, O Governo do Estado do Rio de Janeiro também implementou projeto-piloto de videomonitoramento por reconhecimento facial. Este projeto envolveu a instalação de câmeras no bairro de Copacabana, durante o carnaval, além dos entornos do estádio do Maracanã e do Aeroporto Santos Dumont<sup>8</sup>.

<sup>4</sup> ALENCAR, Itana. **Com mais de mil prisões na BA, sistema de reconhecimento facial é criticado por ‘racismo algorítmico’; inocente ficou preso por 26 dias**. Título G1. Disponível em: <<https://g1.globo.com/ba/bahia/noticia/2023/09/01/com-mais-de-mil-prisoas-na-ba-sistema-de-reconhecimento-facial-e-criticado-por-racismo-algoritmico-inocente-ficou-presos-por-26-dias.ghtml>>. Acesso em: 04 de março de 2024.

<sup>5</sup> BRASIL DE FATO. **Jovem negro acusado por reconhecimento facial é inocentado pela terceira vez**. Tilt BRASIL DE FATO. Disponível em: <<https://www.brasildefato.com.br/2023/10/06/rj-jovem-negro-acusado-por-reconhecimento-facial-e-inocentado-pela-terceira-vez>>. Acesso em: 17 de março de 2024.

<sup>6</sup> NUNES, Pablo; LIMA, Thallita G. L.; RODRIGUES, Yasmin. **Das planícies ao planalto: como Goiás influenciou a expansão do reconhecimento facial na segurança pública brasileira**. Rio de Janeiro: CESeC, 2023, p. 6.

<sup>7</sup> Ibidem, p. 6.

<sup>8</sup> NUNES, Pablo; LEMGRUBER, Julita; RODRIGUES, Yasmin; SILVA, Mariah. **Um Rio de câmeras com olhos seletivos: uso do reconhecimento facial pela polícia fluminense**. Rio de Janeiro: CESeC, 2022, p. 5.



De acordo com a pesquisa “Um Rio de câmeras com olhos seletivos”, a favela do Jacarezinho, na Zona Norte do Rio – que foi o cenário da ação policial mais letal no Rio de Janeiro em 2021 – foi utilizada como laboratório de implantação de câmeras de videovigilância de reconhecimento biométrico<sup>9</sup>. A implementação ocorreu sem a realização de estudos prévios para avaliar os potenciais riscos e impactos para os cidadãos, especialmente em relação aos vieses raciais do uso dessa nova tecnologia<sup>10</sup>.

Ao analisar o uso massivo do reconhecimento facial, bem como o processo de ebulição do uso de Inteligência Artificial (IA) no contexto brasileiro para as mais diversas finalidades, não apenas para a segurança pública, verifica-se a necessidade, cada vez mais expressiva, de debater sobre ética, racismo, riscos e impactos das novas tecnologias, pois apesar da nítida relevância desses tópicos, a discussão ainda não apresenta tanta tração no Brasil, especialmente no âmbito do setor privado.

Mecanismos de policiamento preditivo<sup>11</sup>, como os softwares de reconhecimento facial, não por acaso, repetem padrões perversos de atuação da polícia tanto em relação à hipervigilância do cotidiano quanto em relação aos sujeitos – normalmente corpos negros e periféricos – encurralados neste processo.

Refletir sobre os vieses raciais no uso de tecnologias não deve ser tratado unicamente como uma escolha, mas uma missão cidadã – inclusive de pessoas brancas – para a provocação de mudanças em situações que afetam, de forma direta ou indiretamente, a população negra das violências cometidas pelo passado colonialista e escravocrata.

Moore (2020) aborda que o racismo tem por capacidade moldar-se às mais diversas construções e cenários que perpassam as relações interpessoais e institucionais<sup>12</sup>. Em sua obra, “Racismo e Sociedade: novas bases epistemológicas para entender o racismo”, o autor explora que o racismo já era um elemento fundamental antes da eclosão do capitalismo, porém diante da modernidade capitalista esse fenômeno alastrou-se silenciosamente, desenhando novos tipos de relações sociais.

---

<sup>9</sup> NUNES, Pablo; LEMGRUBER, Julita; RODRIGUES, Yasmin; SILVA, Mariah. **Um Rio de câmeras com olhos seletivos: uso do reconhecimento facial pela polícia fluminense**. Rio de Janeiro: CESeC, 2022, p. 5.

<sup>10</sup> Ibidem, p. 5.

<sup>11</sup> Os sistemas de policiamento preditivo tem por mote prever a ocorrência de crimes e auxiliar no desenvolvimento de estratégias de segurança pública com base em métodos de vigilância ostensiva. (In: ARRUDA, A. J. P.; RESENDE, A. P. B. A.; FERNANDES, F. A. SISTEMAS DE POLICIAMENTO PREDITIVO E AFETAÇÃO DE DIREITOS HUMANOS À LUZ DA CRIMINOLOGIA CRÍTICA. Direito Público, [S. l.], v. 18, n. 100, 2022, p. 666.). Nesse contexto, modula-se uma sociedade de controle e de que nos fala Deleuze, pois deixamos de olhar para as informações como associadas a indivíduos, e sim como relacionadas entre si dentro de um quadro maior, vinculados a grupos sociais. “É justamente essa amostra ou conjunto de dados que deve ser modulado” nos dispositivos disciplinares de vigilância. (In: COSTA, 2004, p. 165-166)

<sup>12</sup> MOORE, Carlos. **Racismo e sociedade: novas bases epistemológicas para entender o racismo**. Belo Horizonte: Mazza Edições, 200, p. 108-110.

O racismo é um fenômeno facilmente adaptável a várias estruturas, o que não seria diferente no mundo globalizado e investido em revoluções tecnológicas. Nesse sentido, este malgrado fenômeno se tornou mais uma engrenagem comum às estruturas algorítmicas, as quais reproduzem discriminações e enviesamentos.

Além do uso de IA na segurança pública, outros exemplos podem ser facilmente citados no que diz respeito à estruturação de novas tecnologias e suas problemáticas concernentes aos vieses discriminatórios e racistas.

Exemplo bastante difundido pela mídia ocorreu em julho de 2015, quando o Google “taggeou” pessoas negras como “gorilas”. Como justificativa, a plataforma informou que “problemas no reconhecimento de imagens podem ser causados por rostos obscurecidos e de diferentes processamentos de contraste necessários para diferentes tons de pele e iluminação”<sup>13</sup>.

Já em julho de 2018, o sistema *Rekognition*, desenvolvido pela Amazon, foi criticado por combinar 28 membros do Congresso com fotos criminais, sendo 39% pessoas negras, enquanto os erros entre brancos ficaram em 5%<sup>14</sup>.

Em março de 2019, um estudo foi divulgado revelando falha significativa na detecção de pedestres negros por parte de carros autônomos, o que corrobora a presença de viés discriminatório algorítmico no desenvolvimento desses sistemas automatizados<sup>15</sup>.

A IA do Facebook, em junho de 2021, também rotulou vídeo de homens negros como “primatas”. Os usuários que assistiram ao vídeo postado pelo *The Daily Mail* no Reino Unido receberam a mensagem automática da plataforma questionando se eles queriam “continuar assistindo vídeos de primatas”<sup>16</sup>.

Os exemplos acima e tantos outros existentes, demonstram como o debate em questão precisa ser amplificado, revelando, inclusive, a necessidade de estabelecimento de políticas públicas eficientes, que garantam a transparência, responsabilidade dos sistemas de inteligência artificial, cumprimento das legislações vigentes e, acima de tudo, respeito à Constituição, com o objetivo

<sup>13</sup> KASPERKEVIC, Jana. **Google says sorry for racist auto-tag in photo app**. Título The Guardian. Disponível em: <<https://www.theguardian.com/technology/2015/jul/01/google-sorry-racist-auto-tag-photo-app>>. Acesso em: 03 de março de 2024.

<sup>14</sup> FARINACCIO, Rafael. **Reconhecimento facial da Amazon confundiu políticos dos EUA com criminosos**. Título TecMundo. Disponível em: <<https://www.tecmundo.com.br/seguranca/132630-reconhecimento-facial-amazon-confundiu-politicos-eua-criminosos.htm>>. Acesso em: 03 de março de 2024.

<sup>15</sup> VIEIRA, Laís. **Carros autônomos podem atropelar mais pessoas negras do que brancas**. Título R7. Disponível em: <<https://noticias.r7.com/tecnologia-e-ciencia/fotos/carros-autonomos-podem-atropelar-mais-pessoas-negras-do-que-brancas-11032019>>. Acesso em: 03 de março de 2024.

<sup>16</sup> SCHNOOR, Marina. **IA do Facebook rotulou vídeo de homens negros como ‘primatas’; empresa pede desculpas**. Disponível em: <<https://olhardigital.com.br/2021/09/04/internet-e-redes-sociais/ai-facebook-rotulou-video-homens-negros-primatas/#:~:text=Usu%C3%A1rios%20que%20assistiram%20um%C3%ADdeo,segundo%20o%20New%20York%20Times,>>>. Acesso em: 01 de março de 2024.



de assegurar a proteção dos direitos individuais e coletivos e evitar danos de difícil reparação aos titulares afetados<sup>17</sup>.

Faz-se necessário enfrentar as formas de manifestações de violência e estigmas decorrentes ou originados pelo “racismo algorítmico”, termo este que será melhor elucidado no decorrer do presente capítulo. Kremer (2023), neste aspecto, afirma que é preciso garantir o desenvolvimento tecnológico ético, que não alimente opressões sociais apoiados em um discurso de eficiência e neutralidade<sup>18</sup>.

Apesar do comum vínculo dessa tecnologia com a neutralidade, na verdade, os algoritmos – presentes na tecnologia – não fazem do mundo um lugar melhor, nem mais justo. Muito pelo contrário, são criações matemáticas humanas feitas para replicar padrões. E ao serem utilizados em sociedades, que tem intrínseco em seus comportamentos e cultura padrões sexistas e racistas, os algoritmos passam a repetir – e até mesmo criar – arquétipos, mas em escala automatizada.

Diante da problemática exposta, para a estruturação das bases necessárias para o entendimento acerca dos obstáculos do desenvolvimento de tecnologias seguras e justas para a população negra – as quais respeitem a proteção dos seus direitos fundamentais de liberdade e privacidade – este capítulo irá se ater ao entendimento das novas demonstrações do racismo estrutural, as quais decorrem da dataficação da vida<sup>19</sup>, além de analisar as formas de enfrentamento das políticas colonialistas que reforçam as dinâmicas de poder – tanto sociais, quanto raciais – para alcance da consciência política do direito à proteção de dados pelos cidadãos, em específico para a comunidade negra e periférica.

---

<sup>17</sup> LEAL, Mônia Clarissa Hennig; PAULO, Lucas Moreschi. **Algoritmos discriminatórios e jurisdição constitucional: os riscos jurídicos e sociais do impacto dos vieses nas plataformas de inteligência artificial de amplo acesso**. Revista de Direitos e Garantias Fundamentais, v. 24, n. 3, 2023, p. 167.

<sup>18</sup> KREMER, Bianca. **Racismo Algorítmico [Coleção Panorama]**. Org. Thallita G. L. Lima; Pablo Nunes. Rio de Janeiro: CESeC, 2023, p. 9.

<sup>19</sup> De acordo com Lemos (2021), Mayer-Schoenberguer e Cukier (2013) propuseram o termo “datafication” em 2013, para se referirem as formas de modificações de ações, comportamentos e conhecimentos baseados na performance dos dados formulados por sistemas de inteligência algorítmica. Ref.: LEMOS, André. **Dataficação da vida**. Disponível em: <<https://revistaseletronicas.pucrs.br/index.php/civitas/article/view/39638>>. Acesso em: 17 de março de 2024.

# Racismo e Novas Tecnologias: Colonialismo de Dados, Epistemicídio Negro e Racismo Algorítmico

Desde a originalidade do contexto colonial, verifica-se que o que retalha o mundo – antes mesmo das divergências econômicas e diferenças de modos de vida – é o fato de pertencer (ou não) a determinada raça<sup>20</sup>. Nas palavras de Fanon (1968) “nas colônias a infraestrutura econômica é uma superestrutura. A causa é consequência: o indivíduo é rico porque é branco, é branco porque é rico”<sup>21</sup>. Dessa forma, a raça é um aspecto primordial para entendimento das estruturas de poder, estruturas essas que desafiam as narrativas tradicionais de meritocracia e desvendam as camadas de exploração e dominação que perpetuam as desigualdades até os dias atuais.

O processo de resistência dessa velha lógica colonial não se passa despercebido, uma vez que a descolonização ou processo de reversão do pensamento colonial não é resultado de um “poder sobrenatural”. Ao contrário, a libertação deste legado ocorre em processos, de forma gradual, por meio de um ritmo próprio e com muitos entraves a serem superados<sup>22</sup>.

Ao trazer a discussão para os dias atuais, verifica-se que a “velha racialização”<sup>23</sup> colonial” continua a influenciar a sociedade. De acordo com Amadeu da Silveira (2023), o colonialismo moderno é datafocado, em que sua opressão passa, muitas vezes, despercebida, mas sua violência resulta na precarização gradual das condições de trabalho e na submissão social e gamificada das pessoas racializadas não-brancas, moldando os indivíduos à uma nova forma de servidão regida pelos sistemas algorítmicos das corporações dominantes do Norte global<sup>24</sup>.

O termo “datafocado” sugere que o colonialismo moderno estrutura-se na coleta, processamento e na análise de dados como mecanismos essenciais de perpetuação da opressão. Enquanto a “gamificação” pode ser descrita como uma nova configuração de violência, que é moldada por sistemas algorítmicos

<sup>20</sup> FANON, Frantz. **Os condenados da terra**. Editora Civilização Brasileira, 1968, p. 29.

<sup>21</sup> Ibidem, p. 29.

<sup>22</sup> Ibidem, p. 26-27.

<sup>23</sup> Monsma (2013) infere que a racialização é o “processo de essencializar um grupo étnico”, que pode manifestar-se de maneira positiva ou negativa. Segundo o autor, a racialização não implica, de forma automática, em justificativa para a dominação racial. Em contrapartida, o racismo é caracterizado pela ideologia que prega a superioridade de um grupo étnico, atrelado à essencialização negativa do grupo subordinado.

<sup>24</sup> FAUSTINO, Deivison; LIPPOLD, Walter. **Colonialismo digital: por uma crítica hacker-fanoniana**. Boitempo Editorial, 2023, p. 15.



semelhantes aos jogos digitais, onde as pessoas podem ser recompensadas ou punidas pelo seu comportamento e, até mesmo, pela sua forma de existência.

Ainda sobre a opressão gamificada, convém mencionar os sistemas algorítmicos identificados em redes sociais, os quais, por meio da coleta de dados de usuários, podem interferir negativamente no nível de visibilidade de determinado conteúdo e, inclusive, na reputação de indivíduo ou grupo. Para além desse exemplo, é possível mencionar os sistemas de vigilância, os quais realizam o tratamento de dados pessoais – muitas vezes sensíveis – por meio de algoritmos para influenciar comportamentos futuros.

Dessa forma, ainda que este novo colonialismo ocorra de forma sutil, esses novos moldes de dominação não podem ser vistos como menos importantes. Diante desse panorama, cria-se condições para o surgimento do chamado racismo algorítmico, fenômeno que afeta tanto a distribuição de trabalho, quanto ao acesso às tecnologias, o que impacta diretamente na qualidade de vida das pessoas e, até mesmo, na determinação sobre sua sobrevivência<sup>25</sup>.

Kremer (2023) explica que o racismo algorítmico é um fenômeno analítico que examina os aspectos tecnopolíticos dos algoritmos com base na questão racial, levando em consideração também as interseções de gênero, classe social, orientação sexual, deficiência e outras categorias de opressão que podem estar envolvidas. Nesse sentido, o racismo algorítmico pode ser definido como uma forma de discriminação em sistemas tecnológicos ou computacionais perpetuam ou amplificam desigualdades relacionadas às questões raciais.

A referida autora relata que esse fenômeno se manifesta por meio das disparidades políticas, econômicas e jurídicas inerentes ao racismo estrutural, as quais não estão relacionadas à “falibilidades pontuais no uso e produção da tecnologia”<sup>26</sup>.

À vista desse cenário, o presente tópico buscará analisar como a lógica neo-colonial enraizada na sociedade contribui para o surgimento e disseminação do fenômeno explicitado, ou seja, o racismo algorítmico. Visa-se, também, abordar sobre a correlação do tema com a ausência de pessoas negras no debate sobre o uso seguro de IA, além de refletir sobre os mecanismos de enfrentamento do epistemicídio negro no tocante à estruturação e regulamentação de novas tecnologias.

## O Saber Colonial e o Epistemicídio Negro

Silva Rodrigues (2022) menciona que antes os países dominados costumavam fornecer matéria-prima, principalmente bens materiais, para países do Norte global. Agora, essa dinâmica se repete no cenário digital, onde nossos

---

<sup>25</sup> FAUSTINO, Deivison; LIPPOLD, Walter. **Colonialismo digital: por uma crítica hacker-fanoniana**. Boitempo Editorial, 2023, p. 25.

<sup>26</sup> KREMER, Bianca. **Racismo Algorítmico [Coleção Panorama]**. Org. Thallita G. L. Lima; Pablo Nunes. Rio de Janeiro: CESeC, 2023, p. 24.

dados e informações são frequentemente comercializados para empresas de tecnologia sediadas nos centros econômicos e políticos desses países, sem a adequada observância dos direitos dos titulares.

Cassino, Souza e Amadeu da Silveira (2021) argumentam que as tecnologias desenvolvidas nessa lógica neocolonial ou imperialista funcionam com vastas estruturas de coleta e retenção de dados de indivíduos, que geram bilhões de perfis de usuários que são utilizados, posteriormente, para influenciar comportamentos com fins comerciais, ideológicos ou políticos<sup>27</sup>.

Essa lógica – de “extração” de dados do Sul pelo Norte global – representa o chamado “colonialismo de dados”, termo bastante comentado por Ulisses Mejias e Nick Couldry no cenário internacional e, como já citado, por Sérgio Amadeu da Silveira no contexto brasileiro<sup>28</sup>.

Trazer o debate sobre a “racionalização digital”<sup>29</sup> para a comunidade negra, sobretudo para pessoas faveladas e periféricas – a demarcação territorial é essencial neste debate – é lutar contra este pensamento colonial ou alienígena, que se coloca como único, central e válido<sup>30</sup>.

Em pesquisa realizada pelo Instituto Rede Negra em Tecnologia e Sociedade, entre abril e setembro de 2021, foram gerados dados de 113 especialistas negras e negros, das cinco regiões brasileiras, os quais objetivam responder o seguinte questionamento: “Quais são suas Prioridades sobre Antirracismo na Tecnologia / Negritude na Tecnologia?”. As principais prioridades encontradas, ao analisar as dores dos respondentes, foram relativas ao enfrentamento dos temas: 1. Epistemicídio e Invisibilidade dos Conhecimentos; 2. Falta de Diversidade e Inclusão; 3. Inteligência Artificial e Algoritmização; e 4. Vigilância e Violência Estatal<sup>31</sup>.

<sup>27</sup> KREMER, Bianca. **Racismo Algorítmico [Coleção Panorama]**. Org. Thallita G. L. Lima; Pablo Nunes. Rio de Janeiro: CESeC, 2023, p. 8-9.

<sup>28</sup> SILVA, Tarcízio; SILVA, Fernanda dos Santos Rodrigues (orgs.). **Lentes Antirracistas sobre Regulação de Inteligência Artificial**. 2023. Disponível em: <https://desvelar.org/2023/12/12/lentes-antirracistas-sobre-regulacao-de-inteligencia-artificial>. Acesso em: 26 de março de 2024, p. 37.

<sup>29</sup> O conceito de “racionalização digital” perpassa pelo esforço dos estudos sobre colonialismo digital e racismo algorítmico “[...] como tendência de materialização e subjetivação do racismo, não apenas no desenvolvimento da técnica, implícita à composição orgânica do capital, mas sobretudo na distribuição desigual de seu caráter destrutivo”. Ref.: FAUSTINO, Deivison; LIPPOLD, Walter. **Colonialismo digital: por uma crítica hacker-fanoniana**. Boitempo Editorial, 2023., p. 27.

<sup>30</sup> SILVA, Tarcízio; SILVA, Fernanda dos Santos Rodrigues (orgs.). **Lentes Antirracistas sobre Regulação de Inteligência Artificial**. 2023. Disponível em: <https://desvelar.org/2023/12/12/lentes-antirracistas-sobre-regulacao-de-inteligencia-artificial>. Acesso em: 26 de março de 2024, p. 23.

<sup>31</sup> SILVA, Tarcízio; SILVA, Fernanda dos Santos Rodrigues (orgs.). **Lentes Antirracistas sobre Regulação de Inteligência Artificial**. 2023. Disponível em: <https://desvelar.org/2023/12/12/lentes-antirracistas-sobre-regulacao-de-inteligencia-artificial>. Acesso em: 26 de março de 2024, p. 04.



Silva Rodrigues (2023) aborda de maneira crítica sobre a questão do Epistemicídio e Invisibilidade dos Conhecimentos, enfatizando a urgência de superação do apagamento de saberes negros no debate sobre a reprodução do racismo e outras formas de discriminação por meio de novas tecnologias<sup>32</sup>. Essa discussão, contudo, demanda uma revisitação aos argumentos de Silvia Carneiro, a qual se debruça sobre a história do epistemicídio no Brasil, história esta que desqualifica os saberes e excluem sistemática da participação negra no desenvolvimento cultural, político, econômico e social do país.

Carneiro (2005) elucida que o epistemicídio aos afro-descendentes é a história de apagamento do conhecimento negro no Brasil, tendo em vista as circunstâncias de opressões em que o país teve sua origem. Este apagamento, nas palavras da pensadora, “é filho de natural projeto de dominação no Brasil”, que estrutura um sistema complexo de diferentes camadas de poder e privilégios, e que deixa aos africanos e seus descendentes escravizados o fardo da constante exclusão<sup>33</sup>.

Lélia Gonzalez, sobre o tema, enfatiza a necessidade do empoderamento intelectual da comunidade negra, o qual não abrange tão somente a educação formal, mas, também, a compreensão da dinâmica racial na sociedade e a aspiração por uma melhor qualidade de vida<sup>34</sup>.

Destaca-se, nesse sentido, que o apagamento das contribuições negras, afro-centradas e antirracistas sobre tecnologia demarcam as relações de poder e demonstra a realidade como ela é: as tecnologias não são neutras, mas a invisibilidade da população negra obstaculiza a justiça racial e o enfrentamento de séculos de racismo<sup>35</sup>.

<sup>32</sup> SILVA, Rodrigues Fernanda. **“Nada mais sobre nós sem nós”: escurecendo o debate sobre regulamentação de IA no Brasil e pensando mecanismos de combate ao racismo algorítmico.** Disponível em: <[https://www.dropbox.com/sh/ew1kj28o6t9uy22/AAA8niNxazLwMBWWpPqYOs-ha/Fernanda%20dos%20Santos%20Rodrigues%20Silva%20-%20Nombre%20del%20proyecto?-dl=0&preview=%5BVERS%C3%83O+FINAL+PARA+ENVIO%5D+Relat%C3%B3rio+de+Pesquisa.pdf&subfolder\\_nav\\_tracking=1](https://www.dropbox.com/sh/ew1kj28o6t9uy22/AAA8niNxazLwMBWWpPqYOs-ha/Fernanda%20dos%20Santos%20Rodrigues%20Silva%20-%20Nombre%20del%20proyecto?-dl=0&preview=%5BVERS%C3%83O+FINAL+PARA+ENVIO%5D+Relat%C3%B3rio+de+Pesquisa.pdf&subfolder_nav_tracking=1)>. Acesso em: 01 de abril de 2024, p. 6-8.

<sup>33</sup> CARNEIRO, Aparecida Sueli; FISCHMANN, Roseli. **A construção do outro como não-ser como fundamento do ser.** 2005, p. 104.

<sup>34</sup> BARRETO, Raquel de Andrade. **Enegrecendo o feminismo ou feminizando a raça: narrativas de libertação em Angela Davis e Lélia Gonzalez.** Mestrado em História (Dissertação). Pontifícia Universidade Católica do Rio de Janeiro. Rio de Janeiro, 2005. BRIOSCHI, L. R.; TRIGO, M. H. B. Relatos de vida em ciências sociais: considerações metodológicas. Revista Ciência e Cultura, Campinas, SP, v. 39, n. 7.

<sup>35</sup> REDE Negra em Tecnologia e Sociedade. **Prioridades Antirracistas sobre Tecnologia e Sociedade: pesquisa com especialistas negros/os.** Relatório. Ação Educativa, 2021, p. 05.

## A Ausência de Diversidade e Inclusão nos Debates sobre Novas Tecnologias

De forma quase conexas ao apagamento de saberes retratado, frisa-se que a ausência de participação negra no debate sobre a estruturação, desenvolvimento e regulamentação das novas tecnologias também é um ponto de preocupação e evidencia a necessidade de reflexões acerca das implicações econômicas, políticas e sociais advindas desta carência.

Nesse sentido, Cassino, Souza e Amadeu da Silveira (2021) elucidam que o mundo não é “simétrico” e que as tecnologias devem ser analisadas de forma contextual, em respeito às relações históricas e sociais de cada localidade<sup>36</sup> e, para isso, faz-se necessário difundir debates diversos, inclusivos e democráticos.

Reforça-se, então, a necessidade de aumento da presença negra em setores de produção, desenvolvimento, concepção, análise e supervisão de tecnologias. O quadro atual é escasso, prejudicando a existência, tanto de forma individual quanto coletiva, da comunidade negra<sup>37</sup>. O conceito de “racismo por denegação”, sedimentado por Lélia Gonzalez, o qual utiliza base freudiana para descrever a existência de um racismo disfarçado na sociedade brasileira<sup>38</sup> muito explica essa ausência de pessoas racializadas não-brancas neste debate.

Sobre o racismo por denegação, conhecido como uma das formas do racismo estrutural, Kremer (2023) explicita que esta forma de racismo é uma violência, em que, muitas vezes, nem parece uma violência, mas, sim, uma “marca de superioridade” da branquitude. A autora ainda elucida que este tipo de racismo ganhou espaço nas sociedades de origem latina, como a brasileira, em decorrência da prevalência das teorias da miscigenação e do mito da “democracia racial”<sup>39</sup>.

O “racismo por denegação” nada mais é que um “racismo oculto”. Ao transportar a discussão, bem como o conceito supramencionado, para o contexto de desenvolvimento e regulamentação de novas tecnologias no Brasil, é possível observar o seguinte quadro: existe um falso discurso de que a tecnologia será sempre utilizada de forma “positiva” para os cidadãos, inclusive para a população negra; contudo, ainda são poucos os mecanismos eficientes que possibilitem que pessoas negras participem de debates tecnopolíticos e estejam presentes na articulação de políticas públicas sobre o tema.

<sup>36</sup> CASSINO, João; SOUZA, Joyce; DA SILVEIRA, Sérgio Amadeu (Ed.). **Colonialismo de dados: como opera a trincheira algorítmica na guerra liberal**. Autonomia Literária, 2021, p. 08.

<sup>37</sup> REDE Negra em Tecnologia e Sociedade. **Prioridades Antirracistas sobre Tecnologia e Sociedade: pesquisa com especialistas negros/os**. Relatório. Ação Educativa, 2021, p. 05.

<sup>38</sup> KREMER, Bianca. **Racismo Algorítmico [Coleção Panorama]**. Org. Thallita G. L. Lima; Pablo Nunes. Rio de Janeiro: CESeC, 2023, p. 17

<sup>39</sup> Ibidem.



## O fenômeno das “Cidades Inteligentes”, Algoritmização e a Vigilância de Corpos Negros e Periféricos

O projeto das chamadas “*smart cities*” ou “cidades inteligentes”, citado brevemente na introdução deste capítulo – a exemplo do uso de tecnologia na segurança pública e mobilidade urbana – ilustra a “importação” de ideias e tecnologias do Norte global e a necessidade de reflexão sobre os impactos desta integração no cenário brasileiro.

Schiavi (2021) elucida que o termo “*smart cities*” foi adotado por empresas estrangeiras que patrocinam a tendência de dataficação das cidades, por meio de parcerias com órgãos públicos<sup>40</sup>, tendo como pilares mais frequentes desse processo: a valorização de eventos e feiras na cidade; o aprimoramento da mobilidade; e a modernização da segurança pública com uso de tecnologias<sup>41</sup>.

Mendes (2020) menciona que não existem cidades que já tenham implementado este conceito de forma integral, exceto aquelas planejadas para serem construídas do zero, como Songdo, na Coreia do Sul; Masdar, nos Emirados Árabes Unidos; e PlanIT Valley, em Portugal, sendo estas consideradas como projetos a serem desenvolvidos a médio e longo prazo<sup>42</sup>.

Tratando-se do Brasil – país que apresenta grandes problemas relacionados à inclusão digital da população e grandes desigualdades sociais e econômicas – observa-se que o conceito está sendo incorporado de forma pontual, sendo, ainda, distante e uma “tecno-utopia”<sup>43</sup> se pensar na implantação completa de recursos tecnológicos no desenvolvimento urbano.

Uma das maiores críticas ao projeto de “*smart cities*” é a “fetichização da tecnologia”<sup>44</sup>, ou seja, a tendência de idolatria da tecnologia, que assume, de

---

<sup>40</sup> VIA REVISTA UEFSC. **As sete principais críticas à tipologia “cidade inteligente”**. Disponível em: <<https://via.ufsc.br/sete-criticas-cidade-inteligente/#::~:~:text=Dentre%20as%20principais%20raz%C3%B5es%20para,a%20cidade%20inteligente%20C3%A9%20uma>>. Acesso em: 07 de abril de 2024.

<sup>41</sup> Ibidem.

<sup>42</sup> MENDES, Teresa Cristina M. **Smart cities: iniciativas em oposição à visão neoliberal**. Rio de Janeiro: [sn], 2020, p. 2.

<sup>43</sup> Termo utilizado por Mendes (2020) ao descrever a dificuldade de implementação do conceito “*smart cities*”, de forma completa para a maioria das cidades brasileiras.

<sup>44</sup> Nesse sentido, Bell (2011) e Goodspeed (2014) *apud* Tambelli (2014) mencionam que existe uma simplificação dos problemas urbanos a desafios predominantemente técnicos e solucionados por engenharia ou abordagem quantitativa, caracterizando soluções como “tecnoeconômicas” ou tão somente de gestão. Assim, a questão urbana é encarada apenas como uma questão tecnológica, mas não política e social. Ref.: TAMBELLI, Clarice Nassar. **Smart Cities: uma breve investigação crítica sobre os limites de uma narrativa contemporânea sobre cidades e tecnologia**. Disponível em: <[https://itsrio.org/wp-content/uploads/2018/03/clarice\\_tambelli\\_smartcity.pdf](https://itsrio.org/wp-content/uploads/2018/03/clarice_tambelli_smartcity.pdf)>. Acesso em: 07 de abril de 2024.

forma equivocada, a ideia de que sua aplicação representa “progresso”, e que sua adoção massiva pode sanar as mais diversas questões urbanas e converter a cidade, automaticamente, em “inteligente”<sup>45</sup>.

Também são levantadas críticas acerca da ausência de diálogos que levem em consideração a equidade e o debate público sobre questões como: violação de privacidade; falta de inclusão social; e diminuição da liberdade de expressão e democracia. Além disso, o predomínio do setor privado e a influência neoliberal de privilégio dos interesses das elites empresariais são pontos de crítica sobre este projeto<sup>46</sup>.

O Centro de Operações do Rio de Janeiro (COR) – caso concreto bastante veiculado acerca do fenômeno das “*smart cities*” no Brasil – foi estruturado com alta tecnologia, custando 70 milhões para o Estado do Rio, uma vez que foi adotada equipe de 500 funcionários para gerenciar sensores eletrônicos e mais de 1000 câmeras espalhadas pela cidade. O COR foi desenvolvido com a missão de aliviar problemas relacionados a deslizamentos e enchentes, mobilidade, à poluição, ao uso de energia, à violência, entre outros, trazendo como promessa a otimização dos recursos públicos para melhor infraestrutura da cidade<sup>47</sup>.

Contudo, conforme descrito por Tambelli (2014) “[...] embora o COR pudesse ser útil em determinadas situações, o problema raiz motivador do investimento, os deslizamentos de moradias em situação de risco, não foram resolvidos”. Além disso, a autora reforça que problemas como violência e ausência de uso consciente de recursos naturais não podem ser resolvidos somente por meio do emprego de soluções de engenharia tecnológica<sup>48</sup>.

Neste processo, é fácil identificar a população mais afetada: a população negra favelada e periférica, que continua a ter seus direitos sociais negados – sejam eles relacionados à moradia, saúde e segurança – e sua participação apagada neste cenário de desigualdades.

De Figueiredo (2016) infere que em cidades brasileiras – onde as instituições formais e informais contribuem para a segregação racial, econômica, de gênero, social, espacial, dentre outras – a aplicação do modelo de “*smart cities*” pode acabar agravando todas essas desigualdades, acarretando consequências graves

<sup>45</sup> VIA REVISTA UFGO. **As sete principais críticas à tipologia “cidade inteligente”**. Disponível em: <<https://via.ufsc.br/sete-criticas-cidade-inteligente/#:~:text=Dentre%20as%20principais%20raz%C3%B5es%20para,a%20cidade%20inteligente%20%C3%A9%20uma>>. Acesso em: 07 de abril de 2024.

<sup>46</sup> Ibidem.

<sup>47</sup> TAMBELLI, Clarice Nassar. **Smart Cities: uma breve investigação crítica sobre os limites de uma narrativa contemporânea sobre cidades e tecnologia**. Disponível em: <[https://itsrio.org/wp-content/uploads/2018/03/clarice\\_tambelli\\_smartcity.pdf](https://itsrio.org/wp-content/uploads/2018/03/clarice_tambelli_smartcity.pdf)>. Acesso em: 07 de abril de 2024, p. 9.

<sup>48</sup> Ibidem, p. 10.



para a população que está inserida nesse contexto de opressão<sup>49</sup>.

Especificamente no que se refere uso de tecnologia na segurança pública, Silva Rodrigues (2023) reforça o pensamento do referido autor ao argumentar que os sistemas de policiamento preditivo, como o PredPol, trazem enormes preocupações quanto a sua aplicabilidade<sup>50</sup>. Destaca-se que este sistema é uma tecnologia de vigilância urbana e atrelada ao desenvolvimento de modelos de “*smart cities*”.

A autora argumenta que “[...] esses sistemas prometem identificar locais de maior incidência de crimes, mas acabam reiterando e potencializando a violência policial contra lugares majoritariamente habitados por pessoas negras.” Dessa forma, este cenário contribui para a criminalização e encarceramento em massa da comunidade negra e periférica, especialmente no contexto brasileiro<sup>51</sup>.

O modelo urbanístico da “cidade inteligente”, o uso perigoso da inteligência artificial e a algoritmização não podem ser vistos com neutralidade<sup>52</sup>, conforme já mencionado no decorrer deste capítulo e apontado por Kremer (2023) ao tratar sobre o conceito de racismo algorítmico. Nas palavras de De Figueiredo (2016) “[...] a escolha de cada sensor, rotina operacional, valor institucional e foco de programa passa por uma escolha, em última instância, política [...]”.

Assim, é primordial, que a tecnologia, bem como às instituições responsáveis pela implementação desse modelo urbano, considerem a complexa realidade socioeconômica e as profundas desigualdades existentes, as quais apresentam diversos níveis e fatores, nas cidades brasileiras<sup>53</sup>.

---

<sup>49</sup> DE FIGUEIREDO, Gabriel Mazzola Poli. **Cidades inteligentes no contexto brasileiro: a importância de uma reflexão crítica**. Disponível em: <<https://www.anparq.org.br/dvd-enanparq-4/SESSAO%2044/S44-04-FIGUEIREDO.%20G.pdf>>. Acesso em: 10 de abril de 2024, p. 10.

<sup>50</sup> SILVA, Tarcízio; SILVA, Fernanda dos Santos Rodrigues (orgs.). **Lentes Antirracistas sobre Regulação de Inteligência Artificial**. 2023. Disponível em: <<https://desvelar.org/2023/12/12/lentes-antirracistas-sobre-regulacao-de-inteligencia-artificial>>. Acesso em: 26 de março de 2024, p. 51.

<sup>51</sup> Ibidem, p. 51.

<sup>52</sup> DE FIGUEIREDO, Gabriel Mazzola Poli. **Cidades inteligentes no contexto brasileiro: a importância de uma reflexão crítica**. Disponível em: <<https://www.anparq.org.br/dvd-enanparq-4/SESSAO%2044/S44-04-FIGUEIREDO.%20G.pdf>>. Acesso em: 10 de abril de 2024, p. 11.

<sup>53</sup> DE FIGUEIREDO, Gabriel Mazzola Poli. **Cidades inteligentes no contexto brasileiro: a importância de uma reflexão crítica**. Disponível em: <<https://www.anparq.org.br/dvd-enanparq-4/SESSAO%2044/S44-04-FIGUEIREDO.%20G.pdf>>. Acesso em: 10 de abril de 2024, p. 11.

## Enfrentamento ao racismo algorítmico nos debates tecnopolíticos

Para reiterar o que foi discutido neste capítulo, destaca-se que sob manto de um discurso falso de neutralidade da tecnologia, fica evidente o afastamento de pessoas negras dos debates tecno-políticos.

Nesse aspecto, Bhambra (2017) argumenta que a neutralidade técnica é uma maneira de refletir um mundo que não reconhece o papel desempenhado pela raça na própria estruturação das ferramentas tecnológicas<sup>54</sup>. O racismo epistêmico ou a “branquitude metodológica” – é uma associação bastante sutil entre racismo e produção de conhecimento, onde o conhecimento técnico é dito como superior e neutro.

Mbembe (2014) já aduzia, por exemplo, a emergência de um Estado cada vez mais tecnocrático, onde a vigilância opera como “fonte de identificação e de automatização do reconhecimento facial com o objetivo constituir uma nova espécie da população com predisposição para o distanciamento e o enclausuramento”. Nessa linha, a raça é elemento central para a operação e processos descritos por Mbembe, tornando-se um mecanismo de segurança, uma “tecnologia do governo”, adiciona<sup>55</sup>.

Não existe racismo fora de uma relação de poder. A interseção da tecnologia com o poder exerce controle e vigilância sobre os corpos negros, e nesse ponto da discussão faz-se relevante compreender as estratégias de combate ao racismo algorítmico.

Na pesquisa “Prioridades Antirracistas sobre Tecnologia e Sociedade: pesquisa com especialistas negras/os”<sup>56</sup>, a qual já foi mencionada neste capítulo, o Instituto Rede Negra em Tecnologia e Sociedade revela que o combate ao epistemicídio e ao apagamento dos saberes negros emerge como uma prioridade central dentro deste tema.

Entre as medidas de enfrentamento listam-se a promoção de políticas e recursos públicos, a comunicação e educação alternativa, regulação e prestação de contas, a construção de redes para troca de conhecimento, ocupação de espaços, fundos e financiamento, e por fim o ponto mais citado, a produção

<sup>54</sup> BHAMBRA, Gurinder K. **Why are the white working classes still being held responsible for Brexit and Trump?**. LSE Brexit Blog, 2017.

<sup>55</sup> MBEMBE, Achille. **A crítica da razão negra**, 2018, p.38

<sup>56</sup> REDE Negra em Tecnologia e Sociedade. **Prioridades Antirracistas sobre Tecnologia e Sociedade: pesquisa com especialistas negras/os**. Relatório. Ação Educativa, 2021.



de pesquisa e geração de dados<sup>57</sup>.

De maneira análoga, Silva Rodrigues (2023) ressalta a importância de escurecer o debate sobre raça e tecnologia, ecoando a célebre frase: “nada mais sobre nós sem nós”<sup>58</sup>. Dessa forma, é crucial combater o racismo algorítmico<sup>59</sup> com a ocupação ou inclusão ativa, ou seja, por meio do esforço constante para evitar a perpetuação das exclusões, particularmente em discussões que afetam significativamente as vivências da comunidade negra.

Dada a constante mutabilidade do racismo, demanda-se que essa seja uma movimentação contínua de análise e compreensão do funcionamento dessa estrutura a fim de que possa-se delinear estratégias de resistência. Portanto, faz-se relevante racializar e politizar esse enfrentamento com consciência das suas peculiaridades e engrenagens.

Nessa linha, Kremer (2021) destaca a importância do “recentramento racial” como ponto nodal em tecno-regulação e governança algorítmica, conceito pilar para o confronto dessa estrutura. O recentramento racial para a referida intelectual significa “colocar a racialidade no epicentro do debate sobre governança de/por algoritmos sob uma perspectiva de erradicação de sua desumanização e coisificação, mantida pela violência permanente e pelo silenciamento”<sup>60</sup>.

Assim, tendo a consciência política como norte desta empreitada, são diversos os coletivos e entidades que estão atuando nessa frente e se mobilizando ativamente. A consciência política é referida aqui como o afastamento do tecnicismo e explicitando as relações de poder envoltas no debate tecnológico. Em nota de pensar em formas de enfrentamento das problemáticas mencionadas no decorrer deste capítulo, destaca-se algumas iniciativas que têm por objetivo defrontar esse panorama.

<sup>57</sup> Ibidem, p. 8-10.

<sup>58</sup> SILVA, Rodrigues Fernanda. **“Nada mais sobre nós sem nós”: escurecendo o debate sobre regulamentação de IA no Brasil e pensando mecanismos de combate ao racismo algorítmico.** Disponível em: <[https://www.dropbox.com/sh/ew1kj28o6t9uy22/AAA8niNxazLwMBWWpPqYOs-ha/Fernanda%20dos%20Santos%20Rodrigues%20Silva%20-%20Nombre%20del%20proyecto?-dl=0&preview=%5BVERS%C3%83O+FINAL+PARA+ENVIO%5D+Relat%C3%B3rio+de+Pesquisa.pdf&subfolder\\_nav\\_tracking=1](https://www.dropbox.com/sh/ew1kj28o6t9uy22/AAA8niNxazLwMBWWpPqYOs-ha/Fernanda%20dos%20Santos%20Rodrigues%20Silva%20-%20Nombre%20del%20proyecto?-dl=0&preview=%5BVERS%C3%83O+FINAL+PARA+ENVIO%5D+Relat%C3%B3rio+de+Pesquisa.pdf&subfolder_nav_tracking=1)>. Acesso em: 01 de abril de 2024, p. 7.

<sup>59</sup> O termo racismo algorítmico é também cunhado por Tarcízio Silva como “fenômeno diretamente ligado ao problema da dupla opacidade – o módulo pelo qual grupos hegemônicos buscam tanto apresentar a ideia de “neutralidade” na tecnologia quanto dissipar o debate sobre racismo e supremacismo branco no Ocidente” (2022, p. 186).

<sup>60</sup> KREMER, Bianca. **DIREITO E TECNOLOGIA EM PERSPECTIVA AMEFRICANA:** Autonomia, algoritmos e vieses raciais. PUCRio, 2021, p. 256.

## A Campanha “Tire Meu Rosto da Sua Mira”

Considerada uma das principais campanhas de ativismo por direitos digitais no ano de 2022, a campanha “Tire Meu Rosto da Sua Mira”<sup>61</sup> – que foi construída por uma série de organizações da sociedade civil e lançada no Fórum da Internet do Brasil 12 – representa faticamente a luta em busca do banimento total do uso das tecnologias digitais de reconhecimento facial na segurança pública<sup>62</sup>.

A campanha ainda ganhou o prêmio EPIC 2024 *International Privacy Champion Award* pelo trabalho de luta pelo banimento dessas tecnologias, em razão da presença de vieses discriminatórios e o alto risco de ameaça aos direitos individuais e coletivos de grupos minoritários, especialmente as pessoas negras.

Como principais ações, a campanha atuou diretamente com autoridades e legisladores, divulgou cartas abertas e promoveu campanhas educativas sobre os prejuízos do uso do reconhecimento facial na segurança pública.

## O webinar “Racismo na Internet: Evidências para Formulação de Políticas Digitais”

Trazendo a discussão ao âmbito de envolvimento com setor público – visto que não se pode perder de vista que a luta deve ser multissetorial – destaca-se a formulação de algumas ações educativas relevantes relacionadas à disseminação do conhecimento sobre justiça social, raça e tecnologia.

A título de exemplo, cumpre citar a promoção do webinar “Racismo na Internet: evidências para formulação de políticas digitais”, realizado em 2023, pela Secretaria de Comunicação Social da Presidência da República e pelo Ministério da Igualdade Racial<sup>63</sup>.

O webinar, o qual foi transmitido pelo Youtube por meio dos canais dos ministérios, foi fruto da criação do Grupo de Trabalho Interministerial (GTI), instituído no Decreto nº 11.787/2023, pelo Presidente da República Luiz Inácio Lula da Silva. O objetivo central deste GTI é de elaboração do Plano Nacional de Comunicação Antirracista do Governo Federal, tendo o evento ocorrido com a

<sup>61</sup> TIRE MEU ROSTO DA SUA MIRA. **Carta Aberta pelo banimento total do uso das tecnologias digitais de reconhecimento facial na segurança pública.** Disponível em: <<https://tiremeuros-todasuamira.org.br/carta-aberta/>>. Acesso em: 25 de março de 2024.

<sup>62</sup> COALIZÃO DIREITOS NA REDE. **#24 Tire meu Rosto da Sua Mira.** Disponível em: <<https://direitosnarede.org.br/podcast/24-tire-meu-rosto-da-sua-mira/>>. Acesso em: 25 de março de 2024.

<sup>63</sup> BRASIL. Secretaria de Comunicação Social da Presidência da República e Ministério da Igualdade Racial. **Relatório Racismo na Internet: evidências para a formulação de políticas digitais.** SILVA, Ane; SOUZA, Gustavo (coord.). Brasília: Secretaria de Comunicação Social, 2023. Disponível em: <<https://www.gov.br/igualdaderacial/pt-br/assuntos/gti-comunicacaoantirracista/bibliografia>>. Acesso em: 26 de março de 2024.



finalidade de apoiar as atividades do GTI e de fomentar a participação social<sup>64</sup>.

Nesta ação realizada pelo Governo Federal, a diversidade e pluralidade de saberes – temas centrais discutidos ao longo deste capítulo – foram efetivamente respeitadas. Isso se deu por meio da participação de representantes da sociedade civil, pesquisadores, em especial especialistas negros, e comunicadores sociais, o que assegurou uma abordagem ampla e equitativa<sup>65</sup>.

Ainda, no Relatório decorrente do webinar e divulgado pelo mesmo Ministério, o especialista Tarcízio Silva sugere uma série de medidas para enfrentar a concentração e os oligopólios nas tecnologias, incluindo o estímulo a iniciativas de internet diversificada, a promoção da conectividade, a proibição de auto-preferência por empresas de tecnologia e a garantia de portabilidade e interoperabilidade de dados para os usuários<sup>66</sup>.

## O e-book “Construindo Caminhos para a Justiça de Dados no Brasil: o Papel das Defensorias Públicas na Proteção de Dados Pessoais”

Outra ação notória de engajamento junto ao setor público ocorreu por meio da parceria entre algumas Defensorias Públicas do Brasil, a instituição Data Privacy Brasil e a Fundação Ford, a qual se iniciou em 2020.

Após dois anos de trabalho, as referidas instituições publicaram o livro digital “Construindo caminhos para justiça de dados no Brasil: o papel das Defensorias Públicas na proteção de dados pessoais”, e-book este que foi resultado do projeto “Expandindo o papel das Defensorias Públicas na proteção de dados pessoais”<sup>67</sup>.

Ainda sobre o projeto de educação comunitária sobre a função das Defensorias, este nasceu em decorrência do reconhecimento de que estas instituições públicas desempenham papel fundamental no resguardo e na concretização dos direitos dos cidadãos, sejam eles individuais ou coletivos.

Dessa maneira, o Data Privacy Brasil estabeleceu uma relação de “colaboração

<sup>64</sup> Ibidem, p. 6.

<sup>65</sup> BRASIL. Secretaria de Comunicação Social da Presidência da República e Ministério da Igualdade Racial. **Relatório Racismo na Internet: evidências para a formulação de políticas digitais**. SILVA, Ane; SOUZA, Gustavo (coord.). Brasília: Secretaria de Comunicação Social, 2023. Disponível em: <<https://www.gov.br/igualdaderacial/pt-br/assuntos/gti-comunicacaoantirracista/bibliografia>>. Acesso em: 26 de março de 2024, p. 14.

<sup>66</sup> Ibidem, p. 17.

<sup>67</sup> BIONI, Bruno et al. **Construindo caminhos para a justiça de dados no Brasil: O papel das Defensorias Públicas na proteção de dados pessoais**. Disponível em: <<https://www.dataprivacybr.org/wp-content/uploads/2022/06/ebook-defensorias-vf-.pdf>>. Acesso em: 18 de março de 2024.

interinstitucional”<sup>68</sup> com as Defensorias Públicas do país, em especial com a Defensoria Pública do estado do Rio de Janeiro e de São Paulo, com a finalidade de auxiliar na criação de estratégias que colocassem a proteção de dados pessoais como um dos pilares para garantia da justiça social, com foco na mitigação das desigualdades estruturais sofridas pela população brasileira vulnerável<sup>69</sup>.

## A Biblioteca “Tecnologias Digitais e Justiça Racial”

No contexto de elaboração de medidas de enfrentamento ao racismo algorítmico e apagamento da participação negra sobre a temática, cumpre anotar a iniciativa do Ministério da Igualdade Racial, com a divulgação da “Biblioteca sobre Tecnologias Digitais e Justiça Racial”<sup>70</sup>, lançada no ano de 2024. Esta ação visa fortalecer e disseminar a compreensão da sociedade brasileira sobre as diversas manifestações de racismo no âmbito digital.

Conforme explanado na página eletrônica da Biblioteca, este projeto é resultado da curadoria realizada pelo especialista negro Tarcizio Silva, que ofertou um vasto mapeamento bibliográfico sobre justiça racial e tecnologia, com o objetivo de proporcionar maiores discussões e ampliar os debates para a sociedade brasileira.

Nesse sentido, as publicações apresentadas na Biblioteca abordam sobre racismo algorítmico, impactos da inteligência artificial para comunidades negras, ciberativismo, discriminação nas redes sociais, proteção de dados e protagonismo de lideranças negras, dentre outros aspectos relevantes<sup>71</sup>.

## Contribuições sobre Regulação de Inteligência Artificial no Brasil

Para além da formulação de medidas de enfrentamento com viés educacional destinadas diretamente à comunidade, é importante destacar as contribuições regulatórias realizadas pelas organizações de sociedade civil que atuam em defesa aos direitos digitais.

Nesse ponto, menciona-se o “Documento Preto I – Contribuições do Aqualtune

<sup>68</sup> Termo utilizado por Johana K. Monagreda, pesquisadora e líder do projeto da Associação Data Privacy Brasil de Pesquisa, ao manifestar a relação de parceria estabelecida com as Defensorias Públicas brasileiras.

<sup>69</sup> BIONI, Bruno et al. **Construindo caminhos para a justiça de dados no Brasil: O papel das Defensorias Públicas na proteção de dados pessoais**. Disponível em: <<https://www.dataprivacybr.org/wp-content/uploads/2022/06/ebook-defensorias-vf-.pdf>>. Acesso em: 18 de março de 2024.

<sup>70</sup> GOV.BR. Ministério da Igualdade Racial. **Biblioteca sobre Tecnologias Digitais e Justiça Racial**. Disponível em: <<https://www.gov.br/igualdaderacial/pt-br/assuntos/gti-comunicacao-antirracista/biblioteca>>. Acesso em: 18 de março de 2024.

<sup>71</sup> Ibidem.



Lab para o debate sobre regulação de Inteligência Artificial no Brasil”<sup>72</sup>, o qual apresenta críticas sobre as previsões principiológicas do Projeto de Lei nº 21/2020 (PL 21/2020)<sup>73</sup> e critérios a serem observados em propostas de marco legal sobre IA.

O Aqualtune Lab, instituição que elaborou a referida contribuição, é um coletivo jurídico que possui olhar multidisciplinar sobre estudos nas áreas do Direito, Tecnologia e Raça. Dessa forma, o objetivo do coletivo é “racializar discussões em temas como uso de tecnologias no sistema jurídico a exemplo das vigilâncias pública e privada [...] políticas de proteção de dados, identificação biométrica, segurança na internet”<sup>74</sup>, conforme descrito em apresentação contida no referido documento.

Neste documento, o coletivo reforça a necessidade de uma regulamentação explicitamente antirracista, que evidencie o princípio da transparência e questões de responsabilidade; que considere o banimento como medida de eliminação de alto risco de determinadas tecnologias, a exemplo do reconhecimento facial na segurança pública; bem como que entenda a necessidade de classificação de riscos com critérios auditáveis e planos de ação.

Em relação ao Projeto de Lei Substitutivo de Inteligência Artificial (PL 2338/2023), o Aqualtune também emitiu contribuições, desta vez por meio de Nota de Posicionamento. Para a organização, o referido projeto substitutivo falha ao permitir “brechas” para o uso da tecnologia de reconhecimento facial e biométrico em espaços públicos, tendo em vista o potencial lesivo do uso desses sistemas aos direitos fundamentais da população brasileira, especialmente aos grupos minoritários<sup>75</sup>.

---

<sup>72</sup> AQUALTUNE LAB. **Documento Preto I - Contribuições do Aqualtune Lab para o debate sobre regulação de Inteligência Artificial no Brasil**. Disponível em: <<https://aqualtunelab.com.br/wp-content/uploads/2022/11/AQUALTUNELAB-DocumentoPreto-A5-V2-web.pdf>>. Acesso em: 02 de junho de 2024.

<sup>73</sup> Conforme mencionado em matéria divulgada pela Coalizão Direitos na Rede em 2023, os debates sobre regulação de IA não são novos, estes iniciaram em 2020, com a proposição do PL 21-A/2020, de autoria do Deputado Eduardo Bismarck e relatoria da Deputada Luísa Canziani. A tramitação do projeto ocorreu sem ampla participação social e foi alvo de críticas, uma vez que esta regulação inicial não apresentava “[...] proteção efetiva e operacionalização do exercício de direitos, bem como a não definição de obrigações e respectivos instrumentos de governança e um arranjo fiscalizatório”. Ref.: COALIZÃO DIREITOS NA REDE. **Coalizão Direitos na Rede divulga nota técnica sobre o PL 2338/2023 que busca regular a IA**. Disponível em: <<https://direitosnarede.org.br/2023/08/23/coalizacao-direitos-na-rede-divulga-nota-tecnica-sobre-o-pl-2338-2023-que-busca-regular-a-ia/>>. Acesso em: 12 de maio de 2024.

<sup>74</sup> AQUALTUNE LAB. **Documento Preto I - Contribuições do Aqualtune Lab para o debate sobre regulação de Inteligência Artificial no Brasil**. Disponível em: <<https://aqualtunelab.com.br/wp-content/uploads/2022/11/AQUALTUNELAB-DocumentoPreto-A5-V2-web.pdf>>. Acesso em: 02 de junho de 2024.

<sup>75</sup> AQUALTUNE LAB. **Nota de Posicionamento do Aqualtune Lab sobre o Projeto de Lei Substitutivo de Inteligência Artificial (PL nº 2338/2023)**. Disponível em: <<https://aqualtunelab.com.br/na-midia/nota-pl2338>>. Acesso em: 02 de junho de 2024.

Nesse sentido, a organização defende os seguintes pontos: a criação de legislação específica sobre o uso de IA na segurança pública, a qual inclua mecanismos de controle para defender os direitos humanos; a promoção de debate diverso e inclusivo, sendo este debate multiparticipativo; a busca de soluções tecnológicas que auxiliem na área de segurança pública sem ferir os direitos individuais e as liberdades civis<sup>76</sup>.

Outra instituição empenhada a jogar luz sobre os desafios éticos e regulatórios referentes ao uso de IA no Brasil – especialmente no tocante aos debates raciais – e que trouxe contribuições relevantes relacionadas ao PL 21/2020, foi o Instituto de Referência em Internet e Sociedade (IRIS).

O IRIS é um centro de pesquisa que se dedica a “produzir e comunicar conhecimento científico sobre os temas de internet e sociedade, bem como a defender e fomentar políticas públicas que avancem os direitos humanos na área digital”<sup>77</sup>.

Diante disso, a organização divulgou, em primeiro momento, contribuição à Comissão de Juristas do Senado referente ao Marco Legal da Inteligência Artificial (PL 21/2020). Nesta contribuição, são apresentadas observações sobre temas trazidos no projeto, como princípios e objetivos; transparência e explicabilidade; definições; responsabilidade civil; supervisão e revisão humana; gestão de riscos; dentre outros aspectos<sup>78</sup>.

Como principais pontos de críticas ao primeiro projeto regulatório de IA, o centro de pesquisa argumenta a inexistência de mecanismos de fiscalização para garantia da efetividade dos princípios e objetivos da proposta regulatória; frisa a importância de inclusão da Avaliação de Impacto Algorítmico, com o objetivo de avaliar e mitigar os impactos da elaboração e uso de sistemas de decisão automatizados; bem como infere sobre a ausência previsões de limitações vinculativas ao desenvolvimento e uso de sistemas tecnológicos de IA com potencial lesivo aos direitos fundamentais, a exemplo do uso de reconhecimento facial na segurança pública<sup>79</sup>.

Outras organizações também se posicionaram e apresentaram sugestões e críticas referentes à legislação de IA no Brasil, sendo demonstrada a atuação das organizações de sociedade civil que militam pelos direitos humanos não

<sup>76</sup> Ibidem.

<sup>77</sup> IRIS. **Sobre o IRIS**. Disponível em: <<https://irisbh.com.br/sobre-o-iris/>>. Acesso em: 02 de junho de 2024.

<sup>78</sup> IRIS. **Marco Legal da Inteligência Artificial: Contribuição à Comissão de Juristas do Senado**. Disponível em: <<https://irisbh.com.br/wp-content/uploads/2022/06/Marco-Legal-da-Inteligencia-Artificial-Contribuicoes-do-IRIS-a-Comissao-de-Juristas-do-Senado-1.pdf>>. Acesso em: 02 de junho de 2024, p. 3.

<sup>79</sup> IRIS. **Marco Legal da Inteligência Artificial: Contribuição à Comissão de Juristas do Senado**. Disponível em: <<https://irisbh.com.br/wp-content/uploads/2022/06/Marco-Legal-da-Inteligencia-Artificial-Contribuicoes-do-IRIS-a-Comissao-de-Juristas-do-Senado-1.pdf>>. Acesso em: 02 de junho de 2024, p. 9 e 10..



somente em âmbito acadêmico, mas também regulatório e de forma coordenada com o Poder Legislativo.

Para além do escopo de atuação das organizações da sociedade civil, é importante destacar a relevante publicação do Plano Brasileiro de Inteligência Artificial (PBIA) de 2024-2028, que prevê o investimento de R\$ 1,76 bi voltado para o uso de IA na melhoria dos serviços públicos. O plano busca tornar o Brasil um modelo global de eficiência no uso de IA no setor público, com foco também na inclusão social<sup>80</sup>.

O Observatório Brasileiro de Inteligência Artificial (OBIA), criado como Eixo 5 do PBIA, o qual foi divulgado em julho de 2024 pelo Governo Federal, objetiva apoiar o processo regulatório e de governança da IA no Brasil. O OBIA é coordenado pelo NIC.br – entidade civil sem fins lucrativos – e conta com parceria do Centro de Gerenciamento e Estudos Estratégicos (CGEE), a Fundação Sistema Estadual de Análise de Dados (SEADE) e o Centro de Inteligência Artificial da USP (Center for Artificial Intelligence - C4AI), tendo como principais compromissos: promover informações sobre o uso de IA; realizar análise ampla e auxiliar na avaliação dos impactos do uso de novas tecnologias na sociedade; e facilitar a criação de políticas setoriais para implantação de IA éticas e confiáveis<sup>81</sup>.

## A Metodologia Geração Cidadã de Dados (GCD) para Promoção da Participação Social

Quando se trata de conscientização política, ferramentas como a metodologia “Geração Cidadã de Dados” (GCD) desempenham um papel relevante na promoção da participação social nesses espaços de enfrentamento, como uma busca de solução por quem vive o extremo dos dados e seus impactos, uma frente ativa de acesso ao debate público e à formulação de políticas. No bojo dos debates internacionais, essa ferramenta é descrita como “conjunto de metodologias e ações práticas, realizadas por diferentes organizações, coletivos e instituições de modo colaborativo, muitos deles oriundos de favelas e periferias, visando contribuir para a transformação social”<sup>82</sup>.

Com abordagem inovadora e participativa a GCD pode capacitar comunidades a entenderem e se envolverem de maneira significativa com os dados que as

<sup>80</sup> PORTAL GOV.BR. **Novo Plano Brasileiro de Inteligência Artificial prevê o investimento de R\$ 1,76 bi para melhoria de serviços públicos**. Disponível em: <<https://www.gov.br/gestao/pt-br/assuntos/noticias/2024/julho/novo-plano-brasileiro-de-inteligencia-artificial-preve-o-investimento-de-r-1-76-bi-para-melhoria-de-servicos-publicos>>. Acesso em: 27 de setembro de 2024.

<sup>81</sup> OBIA. **Sobre o OBIA**. Organização Brasileira de Inteligência Artificial. Disponível em: <<https://www.obia.nic.br/s/sobre>>. Acesso em: 27 de setembro de 2024.

<sup>82</sup> WIKIFAVELAS. **Geração Cidadã de Dados**. WikiFavelas. Disponível em: <[https://wikifavelas.com.br/index.php/Gera%C3%A7%C3%A3o\\_Cidad%C3%A3\\_de\\_Dados#:~:text=A%20Gera%C3%A7%C3%A3o%20Cidad%C3%A3%20de%20Dados,melhorar%20a%20qualidade%20de%20vida](https://wikifavelas.com.br/index.php/Gera%C3%A7%C3%A3o_Cidad%C3%A3_de_Dados#:~:text=A%20Gera%C3%A7%C3%A3o%20Cidad%C3%A3%20de%20Dados,melhorar%20a%20qualidade%20de%20vida)>. Acesso em: 03 de março de 2024.

afetam<sup>83</sup>, isso é especialmente importante em um contexto onde as tecnologias digitais e algoritmos podem perpetuar e amplificar disparidades existentes. O envolvimento dos cidadãos em vários processos na cadeia de valor dos dados, são cada vez mais reconhecidas como essenciais para ajudar a superar muitos desafios de dados de nossos tempos, promovendo ainda mais valores importantes, como justiça, inclusão, abertura e transparência em estatísticas e políticas públicas<sup>84</sup>, “é ação direta e cidadã em um campo negligente, racista, elitista e machista”<sup>85</sup>.

Em sua essência, a Geração Cidadã de Dados (GCD) é o conjunto de ações que possibilitam aos cidadãos, gerar, recolher e utilizar dados para benefícios de suas comunidades ou coletivos<sup>86</sup>. O data\_labe, em exemplo, listou sete passos que ajudam a basear todos os trabalhos de GCD na entidade, são eles: identificar o problema, delimitar os subtópicos, discutir os limites, selecionar bases de dados auxiliares, engajar as pessoas, estruturar a coleta de dados, comunicar os dados. Em especial, tem por princípio a transparência e a participação dos envolvidos, por isso importa a comunicação desses dados.

Em um contexto de crise e desgaste do conceito de cidadania, a GCD dá espaço para uma atuação ativa, buscando a transformação social através do protagonismo de cidadãos que tiveram historicamente os seus direitos renegados<sup>87</sup>. Concomitante, a metodologia caminha em conjunto com o conceito destacado de Kremer do “recentramento racial” e o enfrentamento do panorama do racismo algorítmico, abarcando uma movimentação ativa e mais inclusiva.

<sup>83</sup> SILVA, Fábio. **Mas o que é geração cidadã de dados?**. Disponível em: <<https://medium.com/data-labe/mas-o-que-%C3%A9-gera%C3%A7%C3%A3o-cidad%C3%A3-de-dados-fdac93c8fd70>>. Acesso em: 02 de junho de 2024.

<sup>84</sup> UNSD. **Collaborative on Citizen Data Overview**. Disponível em: <<https://unstats.un.org/UNSDWebsite/citizen-data/>>. Acesso em: 02 de junho de 2024.

<sup>85</sup> VIEIRA, Gilberto. **Geração Cidadã de Dados: um fazer político**. Disponível em: <<https://medium.com/data-labe/gera%C3%A7%C3%A3o-cidad%C3%A3-de-dados-um-fazer-pol%C3%ADtico-c6b0450babfa>>. Acesso em: 02 de junho de 2024.

<sup>86</sup> MOTA, Polinho; VIEIRA, Gilberto. **Geração Cidadã de Dados: Saiba como desenvolver seu projeto de produção de dados com participação social a partir da metodologia utilizada pelo data\_labe**. Disponível em: <<https://datalabe.org/geracao-cidada-de-dados/>>. Acesso em: 02 de junho de 2024.

<sup>87</sup> Ibidem.



## Conclusão

---

Imbricado nas relações sociais, o racismo perpassou a estrutura digital e facilitou o funcionamento das suas engrenagens em maior volume e alcance com as tecnologias de massa e automatizadas listadas no capítulo. O panorama afeta todas as frentes da vida em sociedade, desde a circulação nas cidades até o afastamento dos espaços de debate e construção que influenciam diretamente esses grupos sociais.

Em verdade, o presente capítulo procurou aprofundar sobre o panorama demonstrando como o racismo imbricado às novas tecnologias têm maiores alcances e impactos, fazendo-se relevante a atuação ativa no enfrentamento ao racismo para garantia da justiça nos debates tecnopolíticos. As novas tecnologias revestidas do discurso tecnosolucionista e estruturada com diversas camadas de opacidade de consentimento remete a diversos riscos sistêmicos. Além disso, a proteção de dados assume um papel crucial nesse contexto, pois as tecnologias de coleta, processamento e armazenamento de informações pessoais amplificam as possibilidades de discriminação e exclusão de grupos já vulnerabilizados. Sem uma adequada proteção, os dados podem ser utilizados para reforçar vieses preexistentes e perpetuar desigualdades estruturais, reforçando sistemas de opressão automatizados. A proteção de dados, portanto, não é apenas uma questão de privacidade individual, mas também de justiça social, garantindo que as tecnologias não sejam ferramentas de perpetuação do racismo e outras formas de discriminação, mas sim meios de construção de uma sociedade mais equitativa e inclusiva.

Nesse sentido, destaca-se que, entre as medidas listadas ao longo do capítulo, a maioria são ações voltadas para a frente educacional, refletindo a necessidade de amadurecimento no debate sobre justiça racial, gestão consciente e cidadã de dados, e a aplicação da Lei Geral de Proteção de Dados (LGPD). A educação desempenha um papel crucial na formação de uma sociedade mais crítica e engajada, capaz de identificar e enfrentar as desigualdades ampliadas pelo uso indiscriminado de tecnologias.

Contudo, para um enfrentamento efetivo, é essencial fortalecer o arcabouço jurídico, garantindo que a legislação acompanhe a evolução tecnológica e proteja de maneira eficiente os direitos dos cidadãos, especialmente de grupos historicamente marginalizados. A LGPD, enquanto marco regulatório, oferece diretrizes importantes, mas é preciso ir além da mera adequação às normas: deve-se assegurar que a gestão de dados seja orientada por princípios de equidade e justiça racial, promovendo maior transparência e responsabilização das práticas automatizadas. No próximo capítulo, *Aplicação da LGPD nas Instituições de Pesquisa que utilizam metodologia Geração Cidadã de Dados*, será explorado como esse fortalecimento jurídico, aliado à gestão consciente de dados, pode contribuir para uma sociedade mais justa e inclusiva, alinhando educação e regulação para transformar o cenário tecnopolítico.

## Referências

ARRUDA, A. J. P.; RESENDE, A. P. B. A.; FERNANDES, F. A. **Sistemas de Policiamento Preditivo e Afetação de Direitos Humanos à luz da Criminologia Crítica**. Direito Público, [S. l.], v. 18, n. 100, 2022. DOI: 10.11117/rdp.v18i100.5978. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/5978>. Acesso em: 23 abr. 2024.

ALENCAR, Itana. **Com mais de mil prisões na BA, sistema de reconhecimento facial é criticado por ‘racismo algorítmico’; inocente ficou preso por 26 dias**. Título G1. Disponível em: <https://g1.globo.com/ba/bahia/noticia/2023/09/01/com-mais-de-mil-prisoas-na-ba-sistema-de-reconhecimento-facial-e-criticado-por-racismo-algoritmico-inocente-ficou-presos-por-26-dias.ghtml>. Acesso em: 04 de março de 2024.

AQUALTUNE LAB. **Documento Preto I - Contribuições do Aqualtune Lab para o debate sobre regulação de Inteligência Artificial no Brasil**. Disponível em: <https://aqualtune-lab.com.br/wp-content/uploads/2022/11/AQUALTUNELAB-DocumentoPreto-A5-V2-web.pdf>. Acesso em: 02 de junho de 2024.

AQUALTUNE LAB. **Nota de Posicionamento do Aqualtune Lab sobre o Projeto de Lei Substitutivo de Inteligência Artificial (PL nº 2338/2023)**. Disponível em: <https://aqualtunelab.com.br/na-midia/nota-pl2338>. Acesso em: 02 de junho de 2024.

BARRETO, Raquel de Andrade. **Enegrecendo o feminismo ou feminizando a raça: narrativas de libertação em Angela Davis e Lélia Gonzalez**. Mestrado em História (Dissertação). Pontifícia Universidade Católica do Rio de Janeiro. Rio de Janeiro, 2005. BRIOSCHI, L. R.; TRIGO, M. H. B. Relatos de vida em ciências sociais: considerações metodológicas. Revista Ciência e Cultura, Campinas, SP, v. 39, n. 7.

BHAMBRA, Gurinder K. **Why are the white working classes still being held responsible for Brexit and Trump?**. LSE Brexit Blog, 2017.

BIONI, Bruno et al. **Construindo caminhos para a justiça de dados no Brasil: O papel das Defensorias Públicas na proteção de dados pessoais**. Disponível em: <https://www.dataprivacybr.org/wp-content/uploads/2022/06/ebook-defensorias-vf-.pdf>. Acesso em: 18 de março de 2024.

BRASIL DE FATO. **Jovem negro acusado por reconhecimento facial é inocentado pela terceira vez**. Tilt BRASIL DE FATO. Disponível em: <https://www.brasildefato.com.br/2023/10/06/rj-jovem-negro-acusado-por-reconhecimento-facial-e-inocentado-pela-terceira-vez>. Acesso em: 17 de março de 2024.

BRASIL. Secretaria de Comunicação Social da Presidência da República e Ministério da Igualdade Racial. **Relatório Racismo na Internet: evidências para a formulação de políticas digitais**. SILVA, Ane; SOUZA, Gustavo (coord.). Brasília: Secretaria de Comunicação Social, 2023. Disponível em: <https://www.gov.br/igualdaderacial/pt-br/assuntos/gti-comunicacaoantirracista/bibliografia>. Acesso em: 26 de março de 2024.

CARNEIRO, Aparecida Sueli; FISCHMANN, Roseli. **A construção do outro como não-ser como fundamento do ser**. 2005, p. 104.



CASSINO, João; SOUZA, Joyce; DA SILVEIRA, Sérgio Amadeu (Ed.). **Colonialismo de dados: como opera a trincheira algorítmica na guerra liberal**. Autonomia Literária, 2021, p. 08.

COALIZÃO DIREITOS NA REDE. **#24 Tire meu Rosto da sua Mira**. Disponível em: <<https://direitosnarede.org.br/podcast/24-tire-meu-rosto-da-sua-mira/>>. Acesso em: 25 de março de 2024.

DE FIGUEIREDO, Gabriel Mazzola Poli. **Cidades inteligentes no contexto brasileiro: a importância de uma reflexão crítica**. Disponível em: <<https://www.anparq.org.br/dvd-enanparq-4/SESSAO%2044/S44-04-FIGUEIREDO,%20G.pdf>>. Acesso em: 10 de abril de 2024, p. 10.

FANON, Frantz. **Os condenados da terra**. Editora Civilização Brasileira, 1968, p. 29.

FARINACCIO, Rafael. **Reconhecimento facial da Amazon confundiu políticos dos EUA com criminosos**. Título TecMundo. Disponível em: <<https://www.tecmundo.com.br/seguranca/132630-reconhecimento-facial-amazon-confundiu-politicos-eua-criminosos.htm>>. Acesso em: 03 de março de 2024.

FAUSTINO, Deivison; LIPPOLD, Walter. **Colonialismo digital: por uma crítica hacker-fanoniana**. Boitempo Editorial, 2023, p. 15.

GOV.BR. Ministério da Igualdade Racial. **Biblioteca sobre Tecnologias Digitais e Justiça Racial**. Disponível em: <<https://www.gov.br/igualdaderacial/pt-br/assuntos/gti-comunicacao-antirracista/biblioteca>>. Acesso em: 18 de março de 2024.

IRIS. **Marco Legal da Inteligência Artificial: Contribuição à Comissão de Juristas do Senado**. Disponível em: <<https://irisbh.com.br/wp-content/uploads/2022/06/Marco-Legal-da-Inteligencia-Artificial-Contribuicoes-do-IRIS-a-Comissao-de-Juristas-do-Senado-1.pdf>>. Acesso em: 02 de junho de 2024, p. 3.

IRIS. **Sobre o IRIS**. Disponível em: <<https://irisbh.com.br/sobre-o-iris/>>. Acesso em: 02 de junho de 2024.

KASPERKEVIC, Jana. **Google says sorry for racist auto-tag in photo app**. Título The Guardian. Disponível em: <<https://www.theguardian.com/technology/2015/jul/01/google-sorry-racist-auto-tag-photo-app>>. Acesso em: 03 de março de 2024.

KREMER, Bianca. **DIREITO E TECNOLOGIA EM PERSPECTIVA AMEFRICANA**: Autonomia, algoritmos e vieses raciais. PUCRio, 2021, p. 256

KREMER, Bianca. **Racismo Algorítmico [Coleção Panorama]**. Org. Thallita G. L. Lima; Pablo Nunes. Rio de Janeiro: CESeC, 2023.

LEAL, Mônia Clarissa Hennig; PAULO, Lucas Moreschi. **Algoritmos discriminatórios e jurisdição constitucional: os riscos jurídicos e sociais do impacto dos vieses nas plataformas de inteligência artificial de amplo acesso**. Revista de Direitos e Garantias Fundamentais, v. 24, n. 3, 2023, p. 167.

MBEMBE, Achille. A crítica da razão negra. São Paulo: n-1 edições, 2018.

MENDES, Teresa Cristina M. **Smart cities: iniciativas em oposição à visão neoliberal**. Rio de Janeiro:[sn], 2020, p. 2.

MOORE, Carlos. **Racismo e sociedade: novas bases epistemológicas para entender o racismo**. Belo Horizonte: Mazza Edições, 200, p. 108-110.

MOTA, Polinho; VIEIRA, Gilberto. **Geração Cidadã de Dados: Saiba como desenvolver seu projeto de produção de dados com participação social a partir da metodologia utilizada pelo data\_labe**. Disponível em: <<https://datalabe.org/geracao-cidada-de-dados/>>. Acesso em: 02 de junho de 2024.

NUNES, Pablo; LEMGRUBER, Julita; RODRIGUES, Yasmin; SILVA, Mariah. **Um Rio de câmeras com olhos seletivos: uso do reconhecimento facial pela polícia fluminense**. Rio de Janeiro: CESeC, 2022, p. 5.

NUNES, Pablo; LIMA, Thallita G. L.; RODRIGUES, Yasmin. **Das planícies ao planalto: como Goiás influenciou a expansão do reconhecimento facial na segurança pública brasileira**. Rio de Janeiro: CESeC, 2023, p. 6.

REDE Negra em Tecnologia e Sociedade. **Prioridades Antirracistas sobre Tecnologia e Sociedade: pesquisa com especialistas negras/os**. Relatório. Ação Educativa, 2021, p. 05.

SCHNOOR, Marina. **IA do Facebook rotulou vídeo de homens negros como ‘primatas’; empresa pede desculpas**. Disponível em: <[SILVA, Fábio. \*\*Mas o que é geração cidadã de dados?\*\*. Disponível em: <<https://medium.com/data-labe/mas-o-que-%C3%A9-gera%C3%A7%C3%A3o-cidad%C3%A3-de-dados--fdac93c8fd70>>. Acesso em: 02 de junho de 2024.](https://olhardigital.com.br/2021/09/04/internet-e-redes-sociais/ai-facebook-rotulou-video-homens-negros-primatas/#:~:text=U-su%C3%A1rios%20que%20assistiram%20um%20v%C3%ADdeo,segundo%20o%20New%20York%20Times.></a>>. Acesso em: 01 de março de 2024.</p>
</div>
<div data-bbox=)

SILVA, Rodrigues Fernanda. **“Nada mais sobre nós sem nós”: escurecendo o debate sobre regulamentação de IA no Brasil e pensando mecanismos de combate ao racismo algorítmico**. Disponível em: <[https://www.dropbox.com/sh/ew1kj28o6t9uy22/AAA8niN-xazLwMBWWpPqYOs-ha/Fernanda%20dos%20Santos%20Rodrigues%20Silva%20-%20Nombre%20del%20proyecto?dl=0&preview=%5BVERS%C3%83O+FINAL+PARA+EN-VIO%5D+Relat%C3%B3rio+de+Pesquisa.pdf&subfolder\\_nav\\_tracking=1](https://www.dropbox.com/sh/ew1kj28o6t9uy22/AAA8niN-xazLwMBWWpPqYOs-ha/Fernanda%20dos%20Santos%20Rodrigues%20Silva%20-%20Nombre%20del%20proyecto?dl=0&preview=%5BVERS%C3%83O+FINAL+PARA+EN-VIO%5D+Relat%C3%B3rio+de+Pesquisa.pdf&subfolder_nav_tracking=1)>. Acesso em: 01 de abril de 2024, p. 6-8.

SILVA, Tarcízio; SILVA, Fernanda dos Santos Rodrigues (orgs.). **Lentes Antirracistas sobre Regulação de Inteligência Artificial**. 2023. Disponível em: <<https://desvelar.org/2023/12/12/lentes-antirracistassobre-regulacao-de-inteligencia-artificial>>. Acesso em: 26 de março de 2024, p. 37.

SILVA, Tarcízio. **Racismo algorítmico: inteligência artificial e discriminação nas redes digitais**. Edições Sesc. 2022. 223 pg.

TAMBELLI, Clarice Nassar. **Smart Cities: uma breve investigação crítica sobre os limites de uma narrativa contemporânea sobre cidades e tecnologia**. Disponível em: <[https://itsrio.org/wp-content/uploads/2018/03/clarice\\_tambelli\\_smartcity.pdf](https://itsrio.org/wp-content/uploads/2018/03/clarice_tambelli_smartcity.pdf)>. Acesso em: 07 de abril de 2024, p. 9.



TIRE MEU ROSTO DA SUA MIRA. **Carta Aberta pelo banimento total do uso das tecnologias digitais de reconhecimento facial na segurança pública.** Disponível em: <<https://tiremeurostodasuamira.org.br/carta-aberta/>>. Acesso em: 25 de março de 2024.

UNSD. **Collaborative on Citizen Data Overview.** Disponível em: <<https://unstats.un.org/UNSDWebsite/citizen-data/>>. Acesso em: 02 de junho de 2024.

VIA REVISTA UFGSC. **As sete principais críticas à tipologia “cidade inteligente”.** Disponível em: <<https://via.ufsc.br/sete-criticas-cidade-inteligente/#:~:text=Dentre%20as%20principais%20raz%C3%B5es%20para,a%20cidade%20inteligente%20%C3%A9%20uma>>. Acesso em: 07 de abril de 2024.

VIEIRA, Gilberto. **Geração Cidadã de Dados: um fazer político.** Disponível em: <<https://medium.com/data-labe/gera%C3%A7%C3%A3o-cidad%C3%A3-de-dados-um-fazer-pol%C3%ADtico-c6b0450babfa>>. Acesso em: 02 de junho de 2024.

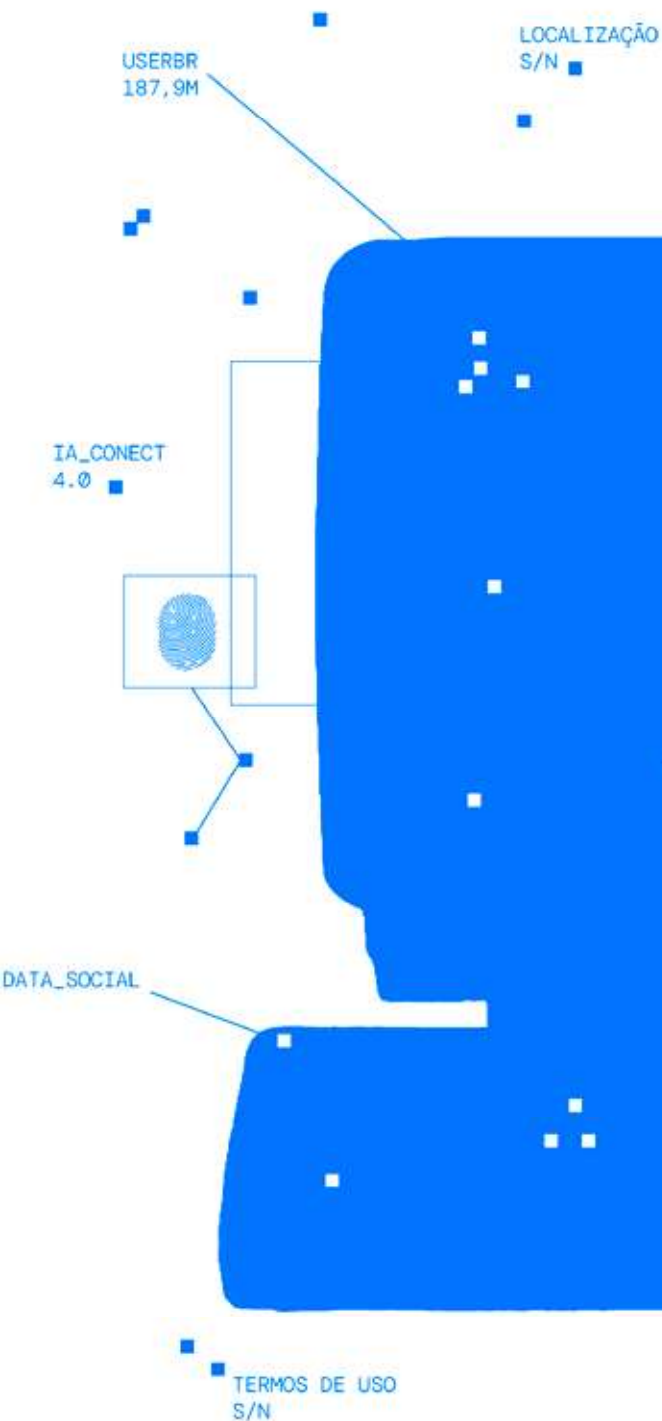
VIEIRA, Laís. **Carros autônomos podem atropelar mais pessoas negras do que brancas.** Título R7. Disponível em: <<https://noticias.r7.com/tecnologia-e-ciencia/fotos/carros-autonomos-podem-atropelar-mais-pessoas-negras-do-que-brancas-11032019>>. Acesso em: 03 de março de 2024.

WIKIFAVELAS. **Geração Cidadã de Dados.** WikiFavelas. Disponível em: [https://wikifavelas.com.br/index.php/Gera%C3%A7%C3%A3o\\_Cidad%C3%A3\\_de\\_Dados#:~:text=A%20Gera%C3%A7%C3%A3o%20Cidad%C3%A3%20de%20Dados,melhorar%20a%20qualidade%20de%20vida](https://wikifavelas.com.br/index.php/Gera%C3%A7%C3%A3o_Cidad%C3%A3_de_Dados#:~:text=A%20Gera%C3%A7%C3%A3o%20Cidad%C3%A3%20de%20Dados,melhorar%20a%20qualidade%20de%20vida). Acesso em: 03 de março de 2024.

# APLICAÇÃO DA LGPD NAS INSTITUIÇÕES DE PESQUISA QUE UTILIZAM METODOLOGIA GERAÇÃO CIDADÃ DE DADOS

**Luize Ribeiro**

**Manuela Oliveira**





### **LUIZE RIBEIRO**

Pesquisadora bolsista do CNPq e convidada pelo Instituto Decodifica. Analista de Qualidade de Dados Jurídicos em empresa de tecnologia. Bacharela em Humanidades, com habilitação em Estudos Jurídicos pela Universidade Federal da Bahia (UFBA). Atualmente é estudante de Direito na mesma instituição. Membro do Laboratório de Inovação e Direitos Digitais da UFBA. Egressa da 15a South School on Internet Governance e Escola de Governança da Internet (EGI). Jovem liderança na Governança da Internet pelo Programa Youth Brasil de 2023 e 2024.

### **MANUELA OLIVEIRA**

Compliance Officer e DPO em empresa de tecnologia, com especialização em Direito Digital, Gestão da Inovação e Propriedade Intelectual pela PUC Minas, além de graduação em Direito pela UFBA. Certificada em Compliance Anticorrupção pela LEC e DPO pela EXIN. Co-fundadora e conselheira no Laboratório de Inovação e Direitos Digitais (LABIDD) e pesquisadora no Legal Grounds Institute. Membro no Compliance Women Committee. Atuação em Justiça Social e Racial, Inteligência Artificial, Direito Registral e Proteção de Dados.

## Introdução

Os dados refletem histórias sobre nós: indivíduos, grupos e sociedades. Quanto mais dados pessoais são tratados e tecnologias empregadas, mais perfis são criados e análises e previsões realizadas<sup>88</sup>. Com o avanço da tecnologia, a coleta de dados pessoais tornou-se uma prática comum em diversas áreas, incluindo marketing, saúde e segurança pública. Empresas e governos utilizam esses dados para oferecer sistemas de recomendação, melhorando a eficiência de operações e até mesmo prevendo comportamentos. No entanto, essa prática também levanta preocupações significativas sobre privacidade e segurança.

Na era da informação, o corpo não se limita mais ao aspecto físico e materialmente visível, mas engloba também o conjunto de dados pessoais sobre o indivíduo, formando o que Stefano Rodotà chamou de “corpo eletrônico”<sup>89</sup>. O jurista italiano destaca a importância da proteção de dados pessoais para o exercício da cidadania e como instrumento contra a expansão do monitoramento estatal e o uso indiscriminado de dados por instituições de diversos setores.

Os dados pessoais são continuamente processados nas mais diversas esferas fazendo com que traços de cada um de nós retem armazenados em inúmeros bancos de dados, onde nossa identidade é dissecada e desmembrada. A regulamentação da coleta e do uso de dados pessoais é essencial para proteger os direitos dos cidadãos. Leis como a GDPR na Europa e a Lei Geral de Proteção de Dados Pessoais (LGPD) aprovada em 2018 no Brasil estabelecem diretrizes rigorosas sobre como as informações devem ser tratadas, exigindo transparência, consentimento explícito e medidas de segurança adequadas. Essas leis visam garantir que os dados dos indivíduos sejam protegidos contra acessos não autorizados e usos indevidos, promovendo um ambiente digital mais seguro e confiável.

Com a ascensão da Inteligência Artificial (IA) e em especial das IA generativas<sup>90</sup> treinadas em grandes bases de dados, faz-se necessário assimilar o lugar do consentimento e outras bases legais na consciência manifesta do que acontece com os nossos dados. A relevância da consciência política foi explorada nos outros capítulos do livro e no presente tópico pretende-se afirmar a importância da educação e conhecimento em uma sociedade datificada. Cientes das

<sup>88</sup> TEFFÉ, Chiara Spadaccini de. **Dados pessoais sensíveis: qualificação, tratamento e boas práticas**. Indaiatuba, SP: Editora Foco, 2022.

<sup>89</sup> RODOTÀ, Stefano. **A vida na sociedade da vigilância – a privacidade hoje**. Coord. Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

<sup>90</sup> Conceito que, embora não tenha definição consensual no território nacional e, nem mesmo na comunidade internacional, diz respeito a um “tipo de tecnologia capaz de gerar textos, imagens e outros conteúdos em resposta a solicitações feitas em linguagem comum.” Data Privacy Brasil. 2023, o ano em que o ChatGPT mostrou a IA generativa ao mundo. São Paulo, 2023. Disponível em: <<https://www.dataprivacybr.org/documentos/2023-o-ano-em-que-o-chatgpt-mostrou-a-ia-generativa-ao-mundo/>>. Acesso em: maio. 2024.



camadas de opacidade em que as tecnologias se revestem pode-se ponderar com maior zelo sobre o que consentimos.

Compreendendo a importância e metodologia da Geração Cidadã de Dados (GCD) em se movimentar como uma busca de solução por quem vive o extremo dos dados e seus impactos, uma frente ativa de acesso ao debate público e à formulação de políticas, faz-se relevante destacar como a regulação da LGPD propõe a adequação e as medidas de segurança para a preservação dos dados pessoais.

O presente capítulo será dividido em seis tópicos: Geração Cidadã de Dados e LGPD: intersecção em conceitos; a adequação de instituições de pesquisa do terceiro setor, um breve contexto brasileiro das Instituições Geração Cidadã de Dados quanto a LGPD, as medidas de segurança da informação, administrativas e técnicas.

## **Geração Cidadã de Dados e LGPD: intersecção em conceitos**

---

A Geração Cidadã de Dados (GCD) ao incentivar a coleta e utilização de dados pelos próprios cidadãos precisa necessariamente alinhar-se com as diretrizes da LGPD. Isso se dá porque, ao manusear dados, especialmente dados pessoais, as iniciativas de GCD devem garantir que os princípios de proteção de dados sejam rigorosamente seguidos. O respeito à privacidade e a garantia de segurança no tratamento dos dados coletados são fundamentais para evitar violações e para promover um ambiente de confiança e respeito mútuo.

Nesse sentido, as iniciativas de GCD devem incorporar práticas que assegurem a conformidade com a LGPD. Por exemplo, ao identificar problemas e delimitar subtópicos, é crucial realizar uma análise de impacto de privacidade, avaliando como os dados serão utilizados e os riscos associados. Na etapa de engajamento das pessoas, é vital obter consentimento explícito e informado dos participantes, explicando claramente como seus dados serão coletados, usados e protegidos.

Além disso, a comunicação dos dados, um dos princípios centrais da GCD, deve ser feita de maneira transparente, garantindo que os dados divulgados não comprometam a privacidade dos indivíduos. Isso inclui a anonimização de dados sempre que possível e a implementação de medidas de segurança robustas para proteger os dados armazenados e transmitidos.

Destarte faz-se necessário compreender a aplicação da Lei Geral de Proteção de Dados (LGPD) às instituições que atuam no terceiro setor junto com a metodologia GCD aprofundando sobre os aspectos técnicos da adequação, pensando nas especificidades dessas organizações.

## Tratamento de dados pessoais para fins acadêmicos x Tratamento de dados pessoais a realização de estudos para órgãos de pesquisa: qual é a diferença para a LGPD?

A Lei Geral de Proteção de Dados (LGPD) estabelece diretrizes específicas para o tratamento de dados pessoais, considerando o contexto e a finalidade do tratamento. Quando falamos em tratamento de dados pessoais para fins acadêmicos e para a realização de estudos por órgãos de pesquisa, existem nuances importantes que diferenciam essas atividades conforme a LGPD.

A Autoridade Nacional de Proteção de Dados (ANPD) publicou estudo técnico<sup>91</sup> que trata sobre essas diferenças, visando fomentar e subsidiar a tomada de decisão sobre o tema tratamento de dados pessoais para fins acadêmicos e realização de estudos por órgão de pesquisa.

De acordo com o art. 4º, II, b, a LGPD não se aplica ao tratamento de dados pessoais realizado para fins exclusivamente acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 da mesma lei. O estudo técnico da ANPD é didático ao mostrar que as distinções se referem às finalidades, bases legais e exigências específicas para a proteção dos dados pessoais envolvidos em cada contexto.

O tratamento de dados pessoais para fins acadêmicos geralmente envolve instituições de ensino, pesquisadores, e estudantes que coletam e utilizam dados pessoais no âmbito de projetos de pesquisa científica, teses, dissertações, e outras atividades acadêmicas. A base legal para este tratamento é frequentemente o consentimento dos titulares dos dados, especialmente quando os dados são sensíveis, com a devida anonimização dos dados e adoção de medidas de segurança para garantir a segurança dos dados e a confidencialidade das informações.

Enquanto que o tratamento de dados pessoais por órgãos de pesquisa, que podem incluir tanto entidades públicas quanto privadas, têm suas próprias particularidades como a finalidade que inclui o desenvolvimento de políticas públicas, inovação tecnológica, e análises estatísticas. Sendo assim, esses órgãos devem observar diretrizes específicas para a proteção dos dados, muitas vezes estabelecidas por comitês de ética e conformidade com normas regulatórias específicas.

Destinchando as diferenças entre ambas destaca-se três pontos: i) consentimento, ii) regulação e fiscalização, e iii) finalidade e escopo. Sobre o consentimento, para fins acadêmicos, esse é mais frequentemente exigido, enquanto que para estudos por órgãos de pesquisa, a LGPD permite o tratamento sem consentimento, desde que os dados sejam anonimizados quando possível.

<sup>91</sup> AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **A LGPD e o tratamento de dados pessoais para fins acadêmicos e para a realização de estudos por órgão de pesquisa**. Brasília: Abril, 2022. Disponível em: <[https://www.gov.br/anpd/pt-br/assuntos/noticias/sei\\_00261-000810\\_2022\\_17.pdf](https://www.gov.br/anpd/pt-br/assuntos/noticias/sei_00261-000810_2022_17.pdf)>. Acesso em: 06 de maio de 2024.



Quanto ao segundo aspecto, os órgãos de pesquisa podem estar sujeitos a regulamentações adicionais e fiscalização por parte de agências reguladoras e comitês de ética, enquanto as instituições acadêmicas seguem diretrizes específicas relacionadas à pesquisa científica. Por fim, o escopo dos estudos realizados por órgãos de pesquisa pode ser mais amplo e incluir finalidades que vão além da pura pesquisa acadêmica, como a elaboração de políticas públicas e desenvolvimento tecnológico.

## Agentes de Tratamento de Dados Pessoais: qual é o papel dos Órgãos de Pesquisa?

Os agentes de tratamento, de acordo com a LGPD, são o controlador e operador de dados pessoais<sup>92</sup>, que podem ser pessoas naturais ou jurídicas, de direito público ou privado<sup>93</sup>.

De acordo com a ANPD, os agentes de tratamento são conhecidos pelo seu “caráter institucional”, ou seja, não são indivíduos subordinados – por exemplo funcionários ou servidores públicos – a uma organização, estes indivíduos subordinados são apenas prepostos destes agentes<sup>94</sup>.

Ressalta-se que os agentes de tratamento são definidos de acordo com a operação de tratamento de dados pessoais. Nesse sentido, a mesma organização pode atuar como controladora ou operadora, conforme a operação de tratamento envolvendo dados pessoais que realizar em determinado momento<sup>95</sup>.

A organização pode ser considerada controladora de dados quando tomar as principais decisões sobre o tratamento de dados pessoais, bem como definir a finalidade deste tratamento<sup>96</sup>. Por outro lado, esta será considerada operadora quando realizar o tratamento em nome da controladora, de acordo com as suas instruções e finalidade por esta delimitada<sup>97</sup>.

Por exemplo, quando uma instituição de pesquisa armazena os dados pessoais

---

<sup>92</sup> **Art. 5º, IX, da LGPD.** Agentes de tratamento: o controlador e o operador.

<sup>93</sup> **Art. 5º, VI, da LGPD.** Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; **Art. 5º, VII, da LGPD.** Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

<sup>94</sup> AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e Encarregado.** Disponível em: <[https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento\\_Final.pdf](https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf)>. Acesso em: 11 de julho de 2024, p. 5.

<sup>95</sup> Ibidem, p. 5.

<sup>96</sup> AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e Encarregado.** Disponível em: <[https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento\\_Final.pdf](https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf)>. Acesso em: 11 de julho de 2024, p. 7.

<sup>97</sup> Ibidem, p. 16.

de participantes de uma pesquisa para um estudo autônomo, a instituição atua como controladora de dados pessoais, uma vez que esta é responsável por estabelecer os elementos essenciais relativos ao tratamento, ou seja, a natureza dos dados pessoais tratados (ex.: os tipos de dados pessoais e a categoria dos titulares) e o período de duração do tratamento (ex.: a definição do período de armazenamento).

Ainda, esta mesma instituição de pesquisa é considerada controladora de dados pessoais ao tratar dados pessoais de seus colaboradores, tendo em vista que a instituição terá o poder de decisão e definirá as finalidades específicas de uso das informações destes titulares (ex.: informações de cunho profissional e de contato).

Por outro lado, no cenário da instituição de pesquisa ser contratada por outra organização – a exemplo de uma universidade – para realizar um estudo e conduzir uma pesquisa acadêmica, a instituição de pesquisa será considerada operadora de dados pessoais, uma vez que a responsabilidade pela definição das finalidades e definição dos meios de tratamento dos dados pessoais coletados para o estudo será a universidade. A instituição de pesquisa apenas seguirá as instruções lícitas e atuará em nome da controladora de dados, neste caso, a universidade.

No tocante à responsabilidade e ressarcimento de danos prevista na LGPD, os agentes de tratamento – o controlador e o operador – que, em razão do exercício de tratamento de dados, causar prejuízo, seja ele de ordem patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados, é obrigado a reparar os envolvidos. Neste caso, a responsabilidade principal será do controlador, enquanto o operador responderá solidariamente pelos danos causados quando descumprir as obrigações da LGPD ou não tiver seguido as instruções lícitas do controlador<sup>98</sup>.

Portanto, verifica-se que as instituições de pesquisa podem atuar tanto como controladoras quanto como operadoras de dados pessoais, dependendo da atividade de tratamento realizada. Essas organizações devem adotar medidas de segurança da informação técnicas e administrativas apropriadas, as quais serão detalhadas ao longo deste capítulo, para garantir o tratamento adequado dos dados pessoais de participantes de pesquisas, colaboradores e parceiros, em conformidade com os dispositivos da LGPD.

---

<sup>98</sup> **Art. 42, da LGPD.** O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. § 1º A fim de assegurar a efetiva indenização ao titular dos dados: I – o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei; II – os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.



# Tratamento de dados pessoais em conformidade com a LGPD em pesquisas

Em respeito à proteção dos participantes de pesquisas e tratamento íntegro de dados, faz-se necessária a atenção dos pontos abaixo para realização de pesquisas envolvendo informações pessoais:

- **Consentimento livre e informado:** É importante que os participantes das pesquisas compreendam e concordem, de forma livre, informada e inequívoca, como será feito o tratamento de seus dados e a finalidade específica para tanto<sup>99</sup>.
- A ANPD menciona que se o tratamento estiver amparado no consentimento, especialmente no âmbito do processamento de dados pessoais para atividades acadêmicas, o controlador deverá observar as seguintes regras estabelecidas na LGPD, tais como: critérios para dispensa de exigência de consentimento (art. 7º, §§ 4º e 6º); necessidade de comunicação ou compartilhamento de dados pessoais com terceiros (art. 7º, § 5º); forma como deve ser dado o consentimento (art. 8º); e direitos dos titulares (art. 9º, §§ 1º e 2º e art. 18)<sup>100</sup>.
- **Segurança da informação:** Conforme será melhor detalhado no decorrer deste capítulo, é de extrema relevância a implementação de medidas de segurança – sejam elas técnicas ou administrativas<sup>101</sup> – com o objetivo de proteger os dados pessoais contra acessos não autorizados, vazamentos e outros tipos de violação de segurança,

<sup>99</sup> **Art. 5º, XII, da LGPD.** Para os fins desta Lei, considera-se: [...] consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

<sup>100</sup> AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia Orientativo para Tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas.** Disponível em: <<https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf>>. Acesso em: 12 de julho de 2024, p. 23.

<sup>101</sup> **Art. 6º, VII, da LGPD.** As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...] segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

nos termos da LGPD<sup>102</sup>.

- Ainda, de acordo com a referida legislação, encontram-se diretrizes específicas para o tratamento de dados pessoais para a realização de estudos por órgãos de pesquisa<sup>103</sup>, abarcando, inclusive, o tratamento de dados pessoais de natureza sensível. Dessa maneira, de acordo com o art. 7º, IV e art. 11, II, c<sup>104</sup>, para a realização de estudos por órgão de pesquisa, deve ser garantida, sempre que possível, a anonimização dos dados pessoais<sup>105</sup>.
- **Transparência:** A LGPD preconiza que as atividades de tratamento deverão observar a boa-fé e o princípio da transparência, isto é, proporcionar garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento envolvidos<sup>106</sup>. O princípio da transparência pode ser materializado por meio de um aviso de privacidade ou, até mesmo, no próprio termo de ciência de tratamento de dados pessoais ou de consentimento.

<sup>102</sup> **Art. 46, da LGPD.** Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

<sup>103</sup> De acordo com a ANPD, “órgãos de pesquisa” apresentam os seguintes requisitos : pessoa jurídica de direito público ou privado sem fins lucrativos; entidades e órgãos públicos ou pessoas jurídicas de direito privado que possuam em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico tecnológico ou estatístico. Ref.: AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia Orientativo para Tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas.** Disponível em: <<https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf>>. Acesso em: 12 de julho de 2024, p. 31.

<sup>104</sup> **Art. 7º, da LGPD.** O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: [...] IV - Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

**Art. 11, da LGPD.** O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: [...] II - sem fornecimento do consentimento do titular, nas hipóteses em que for indispensável para: [...] c) Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis.

<sup>105</sup> AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia Orientativo para Tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas.** Disponível em: <<https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf>>. Acesso em: 12 de julho de 2024, p. 26.

<sup>106</sup> **Art. 6º, da LGPD.** As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...] VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.



- **Necessidade e minimização de coleta de dados:** O princípio da necessidade, disposto na LGPD, considera que o tratamento de dados pessoais deve ser limitado ao mínimo necessário para a realização das finalidades delimitadas pelo agente de tratamento<sup>107</sup>. Dessa maneira, deve-se prezar pela minimização da coleta de informações, ou seja, a instituição de pesquisa deve coletar apenas os dados necessários para o propósito específico da pesquisa, evitando a coleta de dados excessivos ou que não sejam relevantes.
- **Direitos dos titulares de dados pessoais:** Com o advento da LGPD, é fundamental respeitar os direitos dos participantes da pesquisa que confiaram os seus dados pessoais à instituição. A referida lei traz um rol de direitos que os titulares podem solicitar, a exemplo da confirmação da existência de tratamento – inclusive do armazenamento de dados pessoais; acesso aos dados; correção de informações incompletas, inexatas ou desatualizadas, dentre outros. Assim, cabe à instituição de pesquisa verificar como esses direitos podem ser viabilizados, bem como realizar o atendimento, de forma diligente, de seus titulares<sup>108</sup>.

## Dados pessoais sensíveis

Dentro desse contexto, entre todas as várias categorias a que se refere a LGPD, há uma que requer atenção especial: os dados sensíveis. Esses dados são considerados mais críticos, pois podem gerar discriminação, prejuízo ou danos muito graves à privacidade de qualquer pessoa se forem tratados de forma inadequada. É preciso compreender o que são dados sensíveis e como eles se diferenciam dos dados pessoais para garantir a adequação ou a eficácia na proteção dos direitos do indivíduo nos termos da LGPD.

Os dados pessoais referem-se a informações que dizem respeito a uma pessoa física identificada ou identificável. Isso pode estar relacionado a nome, endereço, número de telefone, endereço de e-mail ou qualquer outra informação por meio da qual um indivíduo possa ser identificado indireta ou diretamente<sup>109</sup>.

---

<sup>107</sup> **Art. 6º, da LGPD.** As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...] III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

<sup>108</sup> **Art. 9º, VII, da LGPD.** O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso [...] VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

<sup>109</sup> **Art. 5º, da LGPD.** Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

Por outro lado, os dados sensíveis são considerados informações que podem divulgar detalhes mais íntimos e específicos sobre a vida de uma pessoa. Isso pode incluir origem racial ou étnica, convicções religiosas ou filosóficas, opinião política, filiação a sindicatos, dados relacionados à saúde ou à vida sexual, dados genéticos ou dados biométricos<sup>110</sup>. Essa alta sensibilidade dos dados pode ser colocada em situações como discriminação ou preconceito e outras formas de abuso que afetam seriamente os principais direitos e liberdades do indivíduo em questão.

A previsão dessa categoria específica dos dados sensíveis propõe uma tutela do livre desenvolvimento da personalidade e do princípio da não discriminação, sendo assim explica Teffé que a “compreensão sobre mecanismos que devem ser empregados na tutela de dados sensíveis perpassa um entendimento substancial sobre dinâmicas discriminatórias que estão articuladas nas sociedades”<sup>111</sup>. Isso será aprofundado no próximo tópico sobre os dados pessoais que não estão no rol de sensíveis, mas podem trazer vulnerabilidades aos seus titulares.

O que é relevante na LGPD é a distinção entre dados pessoais e sensíveis para o desempenho de funções que correspondem à pessoa encarregada do tratamento. O tratamento de dados sensíveis deverá ter um caráter de proteção e segurança mais intenso, com consentimento explícito do titular dos dados, medidas técnicas e administrativas especiais para garantir a segurança, acesso somente a pessoas autorizadas e treinadas para trabalhar com esse tipo de informação etc.

Somado a esse fato, a LGPD impõe controles ainda mais rigorosos no tratamento de dados sensíveis, proibindo que eles sejam utilizados para qualquer tipo de finalidade discriminatória, abusiva ou ilícita. Avaliações de impacto envolvendo a proteção de dados também serão necessárias e devem ser conduzidas de forma que medidas para mitigar os riscos associados ao tratamento de dados sensíveis sejam definidas pelas organizações envolvidas no tratamento de informações desse tipo.

Destarte, a diferenciação entre dados pessoais e dados sensíveis, nos termos da LGPD, deixa clara a exigência de uma abordagem mais cuidadosa e rigorosa no tratamento de informações que possam gerar um maior grau de riscos aos quais os titulares dos dados estejam expostos. As medidas de apoio à proteção não significam apenas o cumprimento da lei, mas aumentam a confiança dos titulares de dados nas organizações para manter seguras as informações mais valiosas e pessoais.

<sup>110</sup> **Art. 5º, da LGPD.** Para os fins desta Lei, considera-se: [...] II – dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

<sup>111</sup> TEFFÉ, Chiara Spadaccini de. **Dados Pessoais Sensíveis: qualificação, tratamento e boas práticas**. 2022, p. 19.

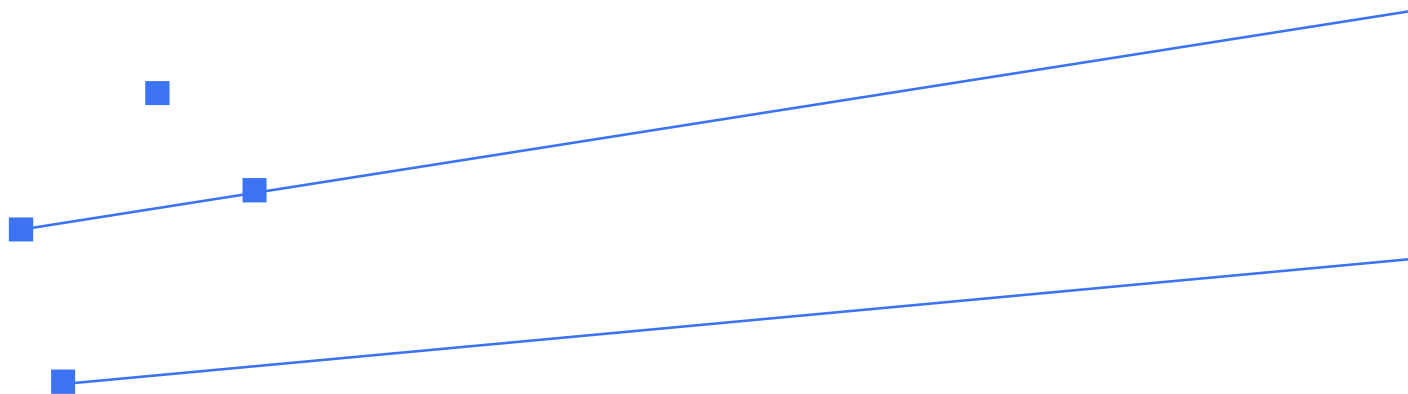
## Dados pessoais que podem trazer vulnerabilidade aos titulares

Ainda que a LGPD traga a definição de dados sensíveis, conforme mencionado no tópico acima, ainda há discussões sobre a taxatividade do rol destes dados.

Alguns doutrinadores defendem a expansividade do conceito de dados sensíveis, sugerindo que o rol apresentado na legislação é exemplificativo. Como fundamento, invocam o princípio da “não discriminação”<sup>112</sup>. Para ilustrar a situação, a geolocalização é citada, pois, por meio do cruzamento de outros dados – ex.: localização de clínicas e laboratórios – pode-se revelar informações de saúde dos titulares<sup>113</sup>.

Já outros doutrinadores entendem que o rol apresentado no art. 5º, II, da LGPD, é taxativo, uma vez que dizer que esse rol é exemplificativo “[...] seria reconhecer que dados como data de nascimento, sexo e salário, também poderiam ser reconhecidos como sensíveis, posto que poderiam conduzir ao etarismo, sexismo e preconceitos sociais, respectivamente [...]”<sup>114</sup>.

Independentemente da corrente adotada, é notório que alguns dados pessoais, ainda que não sejam considerados sensíveis, podem trazer uma vulnerabilidade significativa aos titulares quando expostos de forma indevida, seja pelo alto potencial de causar discriminação ou por propiciarem o comprometimento da segurança dos titulares e, até mesmo, violação indireta dos sigilos bancários destes.



<sup>112</sup> **Art. 6º, da LGPD.** As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...] IX – não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

<sup>113</sup> GUSMÃO, André. **Sobre a taxatividade do rol de dados pessoais sensíveis.** Disponível em: <<https://www.conjur.com.br/2024-jan-13/sobre-a-taxatividade-do-rol-de-dados-pessoais-sensiveis/>>. Acesso em: 16 de junho de 2024.

<sup>114</sup> Ibidem.

Exemplos:

- **Geolocalização:** conforme já mencionado acima, é possível imaginar a situação de uma pesquisa em que coleta dados de geolocalização de pessoas para mapear os lugares frequentados. Caso uma pessoa frequente um hospital especializado em alguma doença crônica, embora o dado de geolocalização não seja sensível, pode-se supor que essa pessoa tem uma doença crônica, expondo-a a discriminação em caso de tratamento irregular destas informações.
- **Dados de renda:** ao imaginar o cenário de coleta de informações sobre o rendimento mensal para análise de padrões de consumo ou entendimento das dificuldades enfrentadas por determinada pessoa, ainda que a renda não seja considerada um dado sensível pela LGPD, a exposição indevida dessa informação pode levar situações de discriminação e, até mesmo, expor o indivíduo e colocar a sua segurança financeira e física em risco.
- **Histórico de compras:** em caso de coleta de dados sobre histórico de compras de indivíduos, com o objetivo de entender seus hábitos de consumo, é preciso estar atento que estas preferências, ainda que não sejam sensíveis, podem ser utilizadas para discriminar determinada pessoa, em caso de vazamento dessas informações.
- **Dados de titulares vulneráveis**<sup>115</sup>: crianças e adolescentes, idosos, pessoas com deficiência, refugiados, empregados e pessoas com doenças graves também merecem atenção especial em seu tratamento, uma vez que estes são considerados grupos vulneráveis e mais suscetíveis a abusos e discriminação. A vulnerabilidade implica que essas pessoas podem não ter a mesma capacidade ou oportunidade para proteger seus próprios interesses em comparação com outros indivíduos.

---

<sup>115</sup> INSTITUTO GLPI. **Tratamento de Dados de Vulneráveis**. Disponível em: <<https://www.glpi.com.br/Infograficos/TRATAMENTO%20DE%20DADOS%20DE%20VULNER%C3%81VEIS.pdf>>. Acesso em: 16 julho de 2024.



## Breve contexto brasileiro das Instituições Geração Cidadã de Dados quanto a LGPD

---

Visando compreender as especificidades das organizações do terceiro setor que atuam com a metodologia GCD quanto à adequação à LGPD, foi proposto um formulário que permitiu identificar alguns padrões relevantes. Embora o contingente analisado seja reduzido e restrito a instituições principalmente no estado do Rio de Janeiro, notou-se uma necessidade urgente de capacitação e suporte técnico para garantir que todas as organizações possam cumprir a LGPD de maneira eficaz, protegendo assim os dados pessoais de seus beneficiários e colaboradores.

De forma breve, ao analisar as respostas do formulário, boa parte das organizações se identifica como periféricas ou compostas por grupos vulnerabilizados, sendo que 71% iniciaram a construção de políticas de privacidade e oferecem medidas de segurança em vigor. Este valor inclui tanto organizações com políticas já implementadas quanto aquelas em processo de implementação. Embora esse seja um número positivo, foram listados diversos desafios para a adequação, como a falta de conhecimento sobre ferramentas e práticas de proteção, a ausência de sistemas adequados, como intranet para operacionalização, além da preocupação significativa com o risco de vazamento de dados, destacando a necessidade de medidas robustas de segurança.

Entre as medidas listadas em comum nas respostas estão a adoção de Política de Segurança da Informação, realização de treinamentos com os membros sobre suas obrigações e responsabilidades, coleta e processamento apenas dos dados pessoais que são realmente necessários para atingir os objetivos do tratamento, estabelecimento de contratos com cláusulas de privacidade e proteção de dados pessoais e a realização de *backups* periódicos e armazenamento de dados de forma segura. Quanto às medidas relativas ao Programa de Privacidade foi recorrente a menção de implementação de Política de Privacidade e a elaboração de Código de Conduta contendo diretrizes sobre privacidade e segurança da informação.

Nesse panorama, é possível afirmar que a adequação à LGPD varia significativamente entre as organizações do terceiro setor. As principais barreiras são a falta de conhecimento e recursos tecnológicos. Há uma necessidade urgente de capacitação e suporte técnico para garantir que todas as organizações possam cumprir a LGPD de maneira eficaz, protegendo assim os dados pessoais de seus beneficiários e colaboradores. Destarte, os próximos tópicos dedicam-se a desenvolver as medidas técnicas para a adequação de forma prática e objetiva.

## Medidas de Segurança da Informação

De acordo com o art. 46 da LGPD, os agentes de tratamento de dados pessoais devem adotar medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Os Órgãos de Pesquisa, por serem considerados agentes de tratamento, também devem implementar salvaguardas que visem proteger as informações contra incidentes de segurança<sup>116</sup> envolvendo dados pessoais.

Frisa-se que instituições que utilizam a metodologia GCD, ainda que, em sua maioria, sejam consideradas agentes de tratamento de pequeno porte<sup>117</sup>, também precisam ter um entendimento básico sobre segurança da informação, uma vez que estas processam dados pessoais – sejam de participantes de pesquisas, corpo de colaboradores e administradores – e enfrentam riscos semelhantes de segurança da informação em comparação aos agentes de tratamento de médio e grande porte<sup>118</sup>.

A segurança da informação é atingida por meio da implementação de um conjunto de controles, que incluem políticas, processos, procedimentos, estruturas organizacionais e, até mesmo, funcionalidades de *software* e *hardware*. Os controles de segurança devem ser estabelecidos, implementados e monitorados de forma contínua, com o objetivo de garantir que os objetivos específicos de segurança e do negócio da organização sejam alcançados<sup>119</sup>.

Como forma de auxílio para diversas organizações, as quais desejam se adequar às melhores práticas de proteção de ativos de informação – sejam estes ativos de cunho pessoal ou não – a ISO/IEC 27002:2013, norma de referência internacional, oferece orientações sobre como realizar a gestão

<sup>116</sup> De acordo com Hintzbergen et. al. (2018), incidente de segurança da informação é definido por um único ou uma série de eventos de segurança da informação indesejados ou não esperados, que possuam probabilidade considerável de comprometer a operação dos negócios e que possam ameaçar a segurança da informação.

<sup>117</sup> O Conselho Diretor da Autoridade Nacional de Proteção de Dados (ANPD) publicou, em 27 de janeiro de 2022, a Resolução CD/ANPD nº 02/2022, a qual dispõe sobre a aplicação da LGPD para agentes de tratamento de pequeno porte. Nos termos da Resolução, os agentes de tratamento de pequeno porte são definidos como microempresas, empresas de pequeno porte, startups, pessoas jurídicas de direito privado, inclusive sem fins lucrativos, nos termos da legislação vigente, bem como pessoas naturais e entes privados despersonalizados que realizam tratamento de dados pessoais.

<sup>118</sup> HINTZBERGEN, Jule et al. **Fundamentos de Segurança da Informação: Com base na ISO 27001 e na ISO 27002**. Brasport, 2018, p. 1.

<sup>119</sup> Ibidem, p. 19.



de segurança da informação. A referida norma é parte da “família” de regulamentos ISO/IEC 27000, que aborda sobre Sistemas de Gestão da Segurança da Informação (SGSI).

Os principais aspectos da ISO/IEC 27002:2013 abarcam: definição de estrutura de governança para a segurança da informação; segurança na área de recursos humanos; gestão de ativos; controle de acesso; uso de criptografia; segurança física e ambiental; segurança operacional; segurança nas comunicações; aquisição, desenvolvimento e manutenção de sistemas; relação com fornecedores; gestão de incidentes de segurança da informação; gestão da continuidade do negócio; e conformidade.

Em âmbito nacional, menciona-se a atuação da ANPD, que em outubro de 2021 publicou o Guia Orientativo de Segurança da Informação para Agentes de Tratamento de Pequeno Porte. O guia em questão traz uma série de boas práticas para estes agentes que, em virtude de seu tamanho e eventuais limitações, muitas vezes não possuem pessoas especializadas em segurança da informação em seu quadro de colaboradores; por outro lado, necessitam aprimorar suas práticas de segurança em relação ao tratamento de dados pessoais, tendo em vista as obrigações contidas nos arts. 46, 47, 48 e 49, da LGPD<sup>120</sup>.

Apesar de ser de extrema relevância o entendimento panorâmico acerca do tema – ou seja, como a segurança da informação é tratada em âmbito internacional e nacional – este trabalho irá se ater à análise das medidas de segurança estipuladas pela ANPD em seu Guia Orientativo para Agentes de Tratamento de Pequeno Porte, uma vez que estas diretrizes abarcam a realidade das instituições de pesquisa que utilizam metodologia GCD já analisadas no presente estudo.

Nesse sentido, serão mencionadas as principais medidas de segurança da informação capazes de promover um ambiente mais seguro para as instituições de pesquisa consideradas agentes de tratamento de pequeno porte, nos termos da LGPD e da Resolução CD/ANPD nº 02/2022<sup>121</sup>.

---

<sup>120</sup> **Art. 46, da LGPD.** Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito;

**Art. 47, da LGPD.** Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término;

**Art. 48, da LGPD.** O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

<sup>121</sup> A Resolução CD/ANPD nº 02/2022 aprovou o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte.

## Medidas de Segurança da Informação Administrativas

As medidas de segurança administrativas são aquelas que se referem ao conjunto de políticas e procedimentos que visam resguardar os dados pessoais. Nesse sentido, a ANPD recomenda a adoção das seguintes medidas administrativas, de acordo com seu guia orientativo, bem como o *checklist* disponível em seu site, que condensa as medidas contidas no referido guia<sup>122</sup>.

### Política de Segurança da Informação

A Política de Segurança da Informação (PSI) é o principal documento de um SGSI<sup>123</sup>. Esta política descreve as diretrizes e regras sobre o planejamento e implementação de controles de segurança da informação numa organização<sup>124</sup>.

A PSI deve ser escrita em conformidade com os requisitos do negócio da organização, levando em consideração as legislações e regulamentos que norteiam a atividade realizada. Recomenda-se que a PSI seja aprovada pelo conselho de administração e divulgada para todo o pessoal da organização, bem como todos os parceiros externos relevantes<sup>125</sup>.

A ISO/IEC 27002:2013 dispõe que a PSI deve ser revisada em intervalos planejados ou em caso de modificação de procedimentos significativos na organização, com o objetivo de assegurar a conformidade, adequação e eficácia do documento<sup>126</sup>.

Embora este documento não seja obrigatório, a ANPD incentiva a sua elaboração e implementação, uma vez que este documento evidencia boa-fé e diligência na segurança dos dados pessoais sob guarda da organização, além de oferecer regras para o funcionamento da gestão de segurança da informação para todos os níveis hierárquicos<sup>127</sup>.

<sup>122</sup> GOV.BR. **ANPD publica Guia de Segurança da Informação para Agentes de Tratamento de Pequeno Porte**. Disponível em: <<https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-guia-de-seguranca-para-agentes-de-tratamento-de-pequeno-porte>>. Acesso em: 29 de junho de 2024.

<sup>123</sup> HINTZBERGEN, Jule et al. **Fundamentos de Segurança da Informação: Com base na ISO 27001 e na ISO 27002**. Brasport, 2018, p. 47.

<sup>124</sup> AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia Orientativo de Segurança da Informação para Agentes de Tratamento de Pequeno Porte**. Disponível em: <<https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf>>. Acesso em: 29 de junho de 2024, p. 8.

<sup>125</sup> HINTZBERGEN, Jule et al. **Fundamentos de Segurança da Informação: Com base na ISO 27001 e na ISO 27002**. Brasport, 2018, p. 67.

<sup>126</sup> Ibidem, p. 69.

<sup>127</sup> AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia Orientativo de Segurança da Informação para Agentes de Tratamento de Pequeno Porte**. Disponível em: <<https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf>>. Acesso em: 29 de junho de 2024, p. 8.



Assim, a ANPD sugere que para agentes de tratamento de pequeno porte, seja estabelecida uma PSI simplificada, a qual abarque os seguintes itens: revisão periódica; e controles relacionados ao tratamento de dados pessoais (ex.: cópias de segurança; uso de senhas; acesso à informação; compartilhamento de dados; atualizações de *softwares*; uso de e-mails; uso de antivírus; entre outros)<sup>128</sup>.

## **Ações de Conscientização**

A ANPD sugere que os agentes de tratamento de pequeno porte conscientizem seus colaboradores para garantir que as diretrizes de segurança da informação sejam cumpridas. O processo de conscientização pode ser realizado por meio de treinamentos e campanhas sobre as obrigações e responsabilidades no tocante ao tratamento de dados pessoais<sup>129</sup>.

A administração deve garantir que o seu corpo de colaboradores encontra-se habilitado para a aplicar a segurança da informação nos termos da PSI e demais políticas internas relativas ao tratamento de dados<sup>130</sup>.

Nesse sentido, recomenda-se que cursos sobre segurança da informação sejam aplicados a todos os colaboradores no momento da admissão, ou seja, na fase de *onboarding* e apresentação da cultura da instituição<sup>131</sup>.

A ANPD sugere temáticas a serem ministrados nas ações de conscientização, sendo elas<sup>132</sup>:

- Como utilizar controles de segurança dos sistemas de TI relacionados ao trabalho diário;
- Como evitar de se tornarem vítimas de incidentes de segurança cibernéticos, tais como contaminação por vírus ou ataques de phishing, que podem ocorrer, por exemplo, ao clicar em links recebidos na forma de pop-up de ofertas promocionais ou em links desconhecidos que chegam por e-mail;
- Manter documentos físicos que contenham dados pessoais dentro de gavetas, e não sobre as mesas;

---

<sup>128</sup> Ibidem, p. 8.

<sup>129</sup> Ibidem, p. 9.

<sup>130</sup> HINTZBERGEN, Jule et al. **Fundamentos de Segurança da Informação: Com base na ISO 27001 e na ISO 27002**. Brasport, 2018, p. 77.

<sup>131</sup> Ibidem, p. 77.

<sup>132</sup> AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia Orientativo de Segurança da Informação para Agentes de Tratamento de Pequeno Porte**. Disponível em: <<https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf>>. Acesso em: 29 de junho de 2024, p. 9.

- Não compartilhar logins e senhas de acesso das estações de trabalho;
- Bloquear os computadores quando se afastar das estações de trabalho, para evitar o acesso indevido de terceiros;
- Seguir as orientações da política de segurança da informação (ANPD, 2021, p. 9).

## Elaboração e Revisão de Contratos

A adoção de medidas jurídicas é de extrema relevância para aplicação dos requisitos de segurança da informação e, consequentemente, cumprimento da LGPD. A elaboração de contratos escritos com fornecedores, parceiros e colaboradores que tratam informações pessoais é visto como um mecanismo de reforço ao compromisso de cumprimento das políticas e procedimentos de segurança da organização.

Em relação ao contrato com parceiros e fornecedores, este deve elucidar o papel de ambas as partes em relação ao tratamento de dados pessoais, as obrigações, responsabilidades de cada parte, a orientação acordada em caso de comunicação de incidentes e recebimento de solicitação de titulares, as possíveis sanções em caso de violações envolvendo dados pessoais, entre outras informações relevantes.

Já em relação ao contrato com colaboradores, é importante que este documento disponha sobre os deveres de confidencialidade e a obrigação de cumprimento das políticas internas relativas à proteção de dados pessoais do agente de tratamento. Para além dos deveres mencionados, recomenda-se que os colaboradores estejam cientes dos seus direitos de proteção de dados, nos termos do art. 18, da LGPD, bem como a finalidade de tratamento de seus dados pessoais no âmbito da organização.

A ANPD sugere os seguintes temas a serem mencionados nas cláusulas contratuais relativas à proteção de dados pessoais<sup>133</sup>:

- Regras para fornecedores e parceiros;
- Regras sobre compartilhamentos;
- Relações entre controlador-operador;
- Orientações sobre o tratamento a ser realizado com vedação a tratamentos incompatíveis com as orientações do controlador (ANPD, 2021, p. 10).

<sup>133</sup> AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia Orientativo de Segurança da Informação para Agentes de Tratamento de Pequeno Porte**. Disponível em: <<https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf>>. Acesso em: 29 de junho de 2024, p. 10.



## Política de Uso e Dispositivos Móveis

Com o uso contínuo de dispositivos móveis (ex.: *smartphones* e *laptops*) para fins profissionais, faz-se necessária a adoção de diretrizes específicas para o uso desses dispositivos.

Dessa forma, a organização deve se questionar sobre suas práticas internas, utilizando as seguintes perguntas como norteadoras: é possível utilizar somente dispositivos corporativos para o manuseio de informações da organização? Quais medidas devem ser tomadas com a utilização de dispositivos corporativos? Em caso de impossibilidade do uso de dispositivos estritamente corporativos, como permitir a utilização de dispositivos pessoais de forma segura?

De acordo com a ANPD, é importante que haja a separação entre os dispositivos móveis de uso privado daqueles de uso institucional, uma vez que “[...] dispositivos móveis de uso privado estão sujeitos a mais vulnerabilidades, por exemplo, pelo uso de aplicativos potencialmente inseguros para fins pessoais”<sup>134</sup>.

Em caso de inviabilidade do uso de dispositivos corporativos, a organização deve realizar uma análise de riscos referente ao uso de dispositivos pessoais, inclusive com a adoção de um plano de ação para minimizar os riscos levantados.

Nesse cenário, o *Bring Your Own Device* (BYOD), também conhecido como “traga o seu próprio dispositivo”, pode ser uma das soluções contidas em plano de ação, devendo existir uma política para o BYOD estruturada, bem como a delimitação de medidas técnicas que visem a proteção das informações contidas nos ativos BYOD.

## Medidas de Segurança da Informação Técnicas

As medidas de segurança técnicas são aquelas que se referem ao conjunto de controles tecnológicos que visam o resguardo dos dados. Assim como a ANPD sugere medidas administrativas, medidas técnicas também são sugeridas em seu guia orientativo, bem como no *checklist* disponível em seu site, que condensa as medidas contidas no referido guia<sup>135</sup>.

<sup>134</sup> AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia Orientativo de Segurança da Informação para Agentes de Tratamento de Pequeno Porte**. Disponível em: <<https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf>>. Acesso em: 29 de junho de 2024, p. 16.

<sup>135</sup> GOV.BR. **ANPD publica Guia de Segurança da Informação para Agentes de Tratamento de Pequeno Porte**. Disponível em: <<https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-guia-de-seguranca-para-agentes-de-tratamento-de-pequeno-porte>>. Acesso em: 29 de junho de 2024.

## Controle de Acesso

Os controles de acesso podem ser divididos em dois grupos: controles de acesso lógico, relacionados a sistemas de informações, e controles de acessos físicos.

O controle de acesso lógico objetiva prevenir que pessoas não autorizadas ganhem acesso lógico para manipular informações que tenham valor para a organização<sup>136</sup>. Já o controle de acesso físicos previne que pessoas não autorizadas transitem em ambientes que devem possuir restrição de acesso em decorrência das informações ali alocadas.

De acordo com a ANPD, o controle de acesso consiste em três processos, sendo eles: autenticação, autorização e auditoria<sup>137</sup>. Dessa forma, “[...] a autenticação identifica quem acessa o sistema ou os dados; a autorização determina o que o usuário identificado pode fazer; a auditoria registra o que foi feito pelo usuário”<sup>138</sup>.

Frisa-se, neste contexto, o processo de autorização, que, como já mencionado, consiste num conjunto de permissões. As permissões podem ser simples ou complexas. As simples são caracterizadas pelo direito de ler um determinado arquivo ou alterar um registro num banco de dados; enquanto as complexas podem ser exemplificadas como possuir permissão para realizar pagamentos bancários a fornecedores<sup>139</sup>.

Para existir controle de acesso, é preciso existir a gestão de acesso dos usuários. Para isso, faz-se necessário as seguintes atividades<sup>140</sup>:

- Registro e cancelamento de registro de usuário;
- Provisionamento de acesso de usuário;
- Gestão de direitos de acesso privilegiado;
- Gestão de informações secretas de autenticação de usuários;
- Revisão dos direitos de acesso de usuários;
- Remoção ou ajuste dos direitos de acesso. (HINTZBERGEN, 2018, p. 87).

<sup>136</sup> HINTZBERGEN, Jule et al. **Fundamentos de Segurança da Informação: Com base na ISO 27001 e na ISO 27002**. Brasport, 2018, p. 86.

<sup>137</sup> AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia Orientativo de Segurança da Informação para Agentes de Tratamento de Pequeno Porte**. Disponível em: <<https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf>>. Acesso em: 29 de junho de 2024, p. 10.

<sup>138</sup> Ibidem, p. 10.

<sup>139</sup> HINTZBERGEN, Jule et al. **Fundamentos de Segurança da Informação: Com base na ISO 27001 e na ISO 27002**. Brasport, 2018, p. 87.

<sup>140</sup> Ibidem, p. 87.



A ANPD também sugere que seja implementado, junto ao controle de acesso, políticas e procedimentos internos de administração de senhas. Nesse sentido, adotar somente “senhas fortes” – ou seja, estabelecimento de números e caracteres especiais – para obter acesso aos sistemas; evitar o uso de senhas padronizadas; realizar a alteração regular de senhas; utilizar a autenticação multi-fatores (MFA); e vedar ao compartilhamento de senhas entre colaboradores são medidas eficazes para diminuir as chances de ameaças e riscos de ataques cibernéticos<sup>141</sup>.

Existem diversas formas de controle de acesso lógico, como: controle de acesso discricionário; mandatório; baseado na função; e baseado em reivindicações. Para os agentes de tratamento de pequeno porte, recomenda-se, em especial, o controle de acesso lógico baseado na função, tendo em vista a maior facilidade de gestão da informação por meio da adoção dessa metodologia e a segurança proporcionada.

No Controle de Acesso Baseado na Função (Role-Based Access Control - RBAC), as decisões de acesso estão relacionadas à posição do sujeito na organização<sup>142</sup>.

Por exemplo, com a adoção do RBAC, um colaborador que está trabalhando numa pesquisa, teria a justificativa de acessar as informações relativas ao projeto em decorrência da sua função (ex.: acesso aos dados coletados, entrevistas, gravações, entre outros). Já os administradores da instituição, poderiam ter acesso a um escopo maior de informações relativas à organização (ex.: informações financeiras, dados de colaboradores, dados relacionados aos fornecedores, entre outros).

## Armazenamento Seguro de Dados Pessoais

Além das ações supramencionadas para o armazenamento seguro de dados pessoais, outras medidas podem ser implementadas, como: uso de criptografia, cópias de segurança (*backups*) e arquivo de *logs*.

A criptografia é bastante útil para manter a informação confidencial. Dessa maneira, é importante delimitar o tipo de criptografia a ser utilizada pela organização e as aplicações que terão essa ferramenta. Além disso, as chaves criptográficas devem ser protegidas contra alterações, perda ou destruição, visto que qualquer uma das ações mencionadas podem ocasionar a impossibilidade de acesso às informações<sup>143</sup>.

<sup>141</sup> AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia Orientativo de Segurança da Informação para Agentes de Tratamento de Pequeno Porte**. Disponível em: <<https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf>>. Acesso em: 29 de junho de 2024, p. 11.

<sup>142</sup> HINTZBERGEN, Jule et al. **Fundamentos de Segurança da Informação: Com base na ISO 27001 e na ISO 27002**. Brasport, 2018, p. 92.

<sup>143</sup> HINTZBERGEN, Jule et al. **Fundamentos de Segurança da Informação: Com base na ISO 27001 e na ISO 27002**. Brasport, 2018, p. 95-96.

Em relação aos *backups*, a ANPD recomenda que elas sejam realizadas de forma regular e completa, além de serem armazenadas em locais seguros e distintos dos dispositivos de armazenamento principais. Ainda, recomenda-se que as cópias não sejam feitas de forma *online*, com o objetivo de evitar a perda de dados em casos de ataques maliciosos<sup>144</sup>.

O principal propósito do *backup* é manter a integridade e a disponibilidade das informações. Nesse sentido, as organizações precisam entender como os backups são manipulados em sua realidade concreta. Ou seja: os *backups* são colocados em armários destrancados? Os *backups* são colocados próximos ao servidor com os dados originais? As informações são criptografadas? Quais práticas podemos adotar para melhorar a gestão dos *backups*? Tais questionamentos são de extrema relevância para a elaboração de procedimentos e políticas internas sobre o tema<sup>145</sup>.

No tocante ao registro de eventos (*logs*), este registro nada mais é do que a coleta de atividades do sistema e dos usuários, bem como de exceções, falhas e eventos relacionados à segurança da informação. Reforça-se que não basta apenas coletar os *logs* em sistemas, sendo fundamental a sua análise. Assim, os *logs* devem ser armazenados em local seguro e protegidos contra modificações ou exclusões, devendo-se analisar por quanto tempo os *logs* serão mantidos, quem terá acesso e o que será registrado<sup>146</sup>.

## Segurança das Comunicações

A segurança das comunicações faz-se extremamente necessária nos dias de hoje, uma vez que a maioria das ferramentas de trabalho estão conectadas à rede de *internet*. Existe uma variedade de formas pelas quais o acesso às redes pode ser protegido, tais como uso de certificados digitais, firewalls, sistemas de detecção de intrusão e uso de criptografia para informações em trânsito<sup>147</sup>.

Uma rede privada, conhecida como *Virtual Private Networks* (VPN), permite a troca de informações entre redes que estão em locais distintos, ou seja, geograficamente separadas, como se estivesse na rede sede da organização. Dessa forma, garante-se, com a utilização de VPN, a proteção dos pilares de integridade, autorização e autenticidade das informações enquanto estas são encaminhadas<sup>148</sup>.

<sup>144</sup> AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia Orientativo de Segurança da Informação para Agentes de Tratamento de Pequeno Porte**. Disponível em: <<https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf>>. Acesso em: 29 de junho de 2024, p. 14.

<sup>145</sup> HINTZBERGEN, Jule et al. **Fundamentos de Segurança da Informação: Com base na ISO 27001 e na ISO 27002**. Brasport, 2018, p. 136.

<sup>146</sup> Ibidem, p. 137.

<sup>147</sup> HINTZBERGEN, Jule et al. **Fundamentos de Segurança da Informação: Com base na ISO 27001 e na ISO 27002**. Brasport, 2018, p. 141.

<sup>148</sup> Ibidem, p. 141.



No tocante ao envio de mensagens eletrônicas, a ANPD recomenda a utilização de conexões cifradas (com uso de TLS/HTTPS) ou aplicativos com criptografia fim a fim, tendo em vista a existência de vulnerabilidades no processo de transferência de informações por meio destes veículos de comunicação. Tratando-se de informações que podem causar uma exposição significativa aos titulares envolvidos em caso de incidentes, a ANPD sugere que e-mails ou arquivos sejam cifrados antes do envio<sup>149</sup>.

## Gerenciamento de Vulnerabilidades e Gestão de Incidentes

As organizações também devem realizar o gerenciamento de vulnerabilidades para monitoramento de possíveis ameaças que possam surgir em seus sistemas e aplicativos. Dessa forma, a ANPD recomenda que todos os sistemas e aplicativos utilizados estejam atualizados em suas últimas versões, bem como que se realize a instalação de atualizações de segurança disponíveis pelos desenvolvedores das tecnologias.

De forma prática, os agentes de tratamento de pequeno porte podem implementar antivírus e antimalwares em seus sistemas, especialmente em computadores e laptops, visando a diminuição de ataques maliciosos e, conseqüentemente, tratamento inadequado de dados pessoais, além de atualizarem os softwares, os quais armazenam dados pessoais, sempre com a versão mais recente de medidas de segurança da informação.

Todavia, caso ocorra um incidente de segurança da informação envolvendo dados pessoais, as organizações – ainda que sejam agentes de pequeno porte – precisam estar preparadas para minimizar os riscos e/ou danos que os titulares possam sofrer. Diante disso, é importante a adoção da gestão de incidentes, que objetiva garantir que os incidentes sejam conhecidos e que as medidas adequadas possam ser tomadas em tempo hábil<sup>150</sup>.

Em relação à gestão de incidentes, cumpre destacar que, em 26 de abril de 2024, a ANPD publicou a Resolução nº 15/2024, que aprova o Regulamento de Comunicação de Incidente de Segurança (RCIS). O normativo contém os objetivos de mitigar ou reverter prejuízos; de assegurar a responsabilização e a prestação de contas; de promover a adoção de boas práticas de governança, prevenção e segurança; e de fortalecer a cultura de proteção de dados no Brasil<sup>151</sup>.

<sup>149</sup> AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia Orientativo de Segurança da Informação para Agentes de Tratamento de Pequeno Porte**. Disponível em: <<https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf>>. Acesso em: 29 de junho de 2024, p. 14.

<sup>150</sup> HINTZBERGEN, Jule et al. **Fundamentos de Segurança da Informação: Com base na ISO 27001 e na ISO 27002**. Brasport, 2018, p. 157.

<sup>151</sup> GOV.BR. **ANPD aprova o Regulamento de Comunicação de Incidente de Segurança**. Disponível em: <<https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aprova-o-regulamento-de-comunicacao-de-incidente-de-seguranca>>. Acesso em: 30 de junho de 2024.

## Considerações finais

---

Observada a aplicação da LGPD e seus detalhamentos no que tange a sua implementação técnica e prática, nota-se também os desafios congruentes a esse processo de adequação, em especial, as organizações do terceiro setor que trabalham com a metodologia GCD, vista as barreiras de falta de conhecimento e recursos tecnológicos. O presente capítulo pretendeu facilitar essa trajetória explicitando de forma objetiva as medidas necessárias e emergentes para a construção de políticas de privacidade.

Faz-se relevante destacar como a intersecção entre GCD e LGPD oferece oportunidade única para fortalecer a confiança entre as comunidades e os processos de coleta de dados. Quando as iniciativas de GCD demonstram um compromisso claro com a proteção de dados, elas não apenas cumprem as exigências legais, mas também promovem uma cultura de respeito e responsabilidade. Isso pode incentivar uma participação mais ativa e consciente dos cidadãos, que se sentem seguros e valorizados no processo.

Finalmente, é importante considerar que a conformidade com a LGPD pode ser vista como um elemento facilitador e não como um obstáculo para a GCD. A lei oferece um quadro estruturado que pode ajudar a orientar as práticas de coleta e uso de dados de maneira ética e segura. Portanto, a sinergia entre GCD e LGPD não só é possível como é desejável, promovendo uma sociedade mais justa, inclusiva e transparente.



## Referências

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **A LGPD e o tratamento de dados pessoais para fins acadêmicos e para a realização de estudos por órgão de pesquisa**. Brasília: Abril, 2022. Disponível em: <[https://www.gov.br/anpd/pt-br/assuntos/noticias/sei\\_00261-000810\\_2022\\_17.pdf](https://www.gov.br/anpd/pt-br/assuntos/noticias/sei_00261-000810_2022_17.pdf)>. Acesso em: 06 de maio de 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e Encarregado**. Disponível em: <[https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentes-deTratamento\\_Final.pdf](https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentes-deTratamento_Final.pdf)>. Acesso em: 11 de julho de 2024.

GOV.BR. **ANPD publica Guia de Segurança da Informação para Agentes de Tratamento de Pequeno Porte**. Disponível em: <<https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-guia-de-seguranca-para-agentes-de-tratamento-de-pequeno-porte>>. Acesso em: 29 de junho de 2024.

GUSMÃO, André. **Sobre a taxatividade do rol de dados pessoais sensíveis**. Disponível em: <<https://www.conjur.com.br/2024-jan-13/sobre-a-taxatividade-do-rol-de-dados-pessoais-sensiveis/>>. Acesso em: 16 de junho de 2024.


HINTZBERGEN, Jule et al. **Fundamentos de Segurança da Informação: Com base na ISO 27001 e na ISO 27002**. Brasport, 2018.

INSTITUTO GLPI. **Tratamento de Dados de Vulneráveis**. Disponível em: <<https://www.glpi.com.br/Infograficos/TRATAMENTO%20DE%20DADOS%20DE%20VULNER%C3%81VEIS.pdf>>. Acesso em: 16 julho de 2024.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: seção 1, Brasília, DF, ano 155, n. 157, p. 1, 15 ago. 2018. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)>. Acesso em: 22 de julho de 2024.

RODOTÀ, Stefano. **A vida na sociedade da vigilância - a privacidade hoje**. Coord. Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

TEFFÉ, Chiara Spadaccini de. **Dados pessoais sensíveis: qualificação, tratamento e boas práticas**. Indaiatuba, SP: Editora Foco, 2022.



# A IMPOR- TÂNCIA DA PARTICIPAÇÃO CIDADÃ PARA UMA EFETIVA CULTURA DE PROTEÇÃO DE DADOS

Kayo Moura

Cláudio Mendes

POWER ON  
ONUR55, 6M  
MN

SERAEX  
STT  
M59, 8M

POWER ON

COLOR#1F1412  
BKWM/AGE27081992

SY=7898  
X=45677

MAD DEM  
STD/MRR  
10001001



### **KAYO MOURA**

Mestre em Ciência Política (IESP-UERJ) e graduando em Estatística (ENCE-IBGE). Kayo é coordenador de pesquisa e dados do Instituto Decodifica. Foi analista de dados do projeto de Justiça Hídrica e Energética da Rede Favela Sustentável (RFS) e professor do curso de pesquisa 'Monitorando a Justiça Hídrica e Energética nas Favelas'. Também contou com passagens pela Secretaria de Assistência Social e Direitos Humanos do Governo do Estado do Rio de Janeiro e pela Secretaria de Planejamento da Prefeitura de Niterói.

### **CLÁUDIO MENDES**

Graduado em Direito pela Universidade do Estado do Rio de Janeiro - UERJ; Pós-graduando em Direito Digital pelo Instituto de Tecnologia e Sociedade do Rio (ITS Rio), em parceria com a UERJ; Advogado; Assessor Jurídico do Instituto Decodifica.



## Introdução

As transformações na tecnologia da informação ocorridas no final do século XX e aprofundadas no início do século XXI modificaram profundamente a sociedade em seus mais diversos campos: econômico, cultural, social e político. Um ponto essencial que caracteriza este novo momento é a forma como produzimos, analisamos e valorizamos a informação (em outras palavras “dados”). Essa nova era trouxe consigo a ampliação do acesso a computadores pessoais, à internet banda larga e a redes sem fio. Esse processo possibilitou o desenvolvimento e a progressiva normalização de redes sociais onde os indivíduos passarão a publicar dados pessoais, de forma voluntária, que vão do nome até localização em tempo real.

Tal amontoado de dados coletados produzidos por usuários nas redes e também por uma economia altamente informatizada é vendido e analisado através de técnicas de *big data*<sup>152</sup>, possibilitando que empresas privadas utilizem desde estratégias de marketing focadas em determinado perfil de consumidor até que seja concedido acesso a crédito, por exemplo. Instituições do Estado também se valem desses dados como estopim para prisões e inquéritos que culminam em operações policiais, a exemplo da Chacina do Jacarezinho ocorrida em 6 de maio de 2021 na cidade do Rio de Janeiro<sup>153</sup>. Dessa maneira, pode-se afirmar que a proteção de dados é direito que dá base a outros direitos, dentre outros, como a liberdade de expressão, a dissidência democrática, a privacidade e a autonomia privada.

Se por um lado, é verdade que o Estado e o setor privado têm feito uso desses dados como forma de ampliação de lucros e receitas, mas também de vigilância e controle. Por outro lado, a sociedade civil e os movimentos sociais também têm se mobilizado e feito uso das novas tecnologias e ferramentas da informação em suas estratégias de resistência. O levantamento, análise e uso de dados para reivindicar direitos, realizar denúncias, mobilizar grupos e, em última instância, buscar transformação social é uma realidade mundo afora e tem constituído um verdadeiro movimento global, ainda que não necessariamente articulado e coeso. Este movimento chama-se, neste capítulo, de Geração Cidadã de Dados (GCD).

<sup>152</sup> Que segundo o Instituto de Tecnologia e Sociedade do Rio de Janeiro do Rio (ITS-Rio), “é, literalmente, o conjunto de dados cuja existência só é possível em consequência da coleta massiva de dados que se tornou possível nos últimos anos, graças à onipresença de aparelhos e sensores na vida cotidiana e do número crescente de pessoas conectadas a tais tecnologias por meio de redes acesso em digitais e também de sensores”. Big data no projeto Sul Global. Relatório sobre estudos de caso. Instituto de Tecnologia & Sociedade do Rio. Rio de Janeiro, 2016. Disponível em: <[https://itsrio.org/wp-content/uploads/2017/02/ITS\\_Big-Data\\_PT-BR\\_v4.pdf](https://itsrio.org/wp-content/uploads/2017/02/ITS_Big-Data_PT-BR_v4.pdf)>. Acesso em julho 2024.

<sup>153</sup> Evento que é tido como o mais letal da história do Rio de Janeiro. BARREIRA, Gabriel; BRASIL, Filipe. Disponível em: <<https://g1.globo.com/rj/rio-de-janeiro/noticia/2021/05/06/operacao-no-jacarezinho-rio-tem-numero-recorde-de-mortes.html>>. Acesso em julho de 2024.



A GCD pode ser uma arma contra-hegemônica e um mecanismo de participação social fundamental na “era dos dados”, no entanto, para que seus objetivos sejam alcançados sem vulnerabilizar ainda mais os grupos marginalizados é primordial que este movimento tenha um olhar crítico e criterioso para a proteção dos dados que levanta, coleta, analisa e mobiliza. Caso contrário, a GCD pode expor e fragilizar populações, grupos e territórios marginalizados, para o setor privado e o Estado, contribuindo para ampliar sua marginalização, controle e criminalização.

Nessa conjuntura, o debate em torno da proteção de dados ganha tração, especialmente com a aprovação da Lei Geral de Proteção de Dados (LGPD) no ano de 2018, na forma da Lei nº 13.709, de 14 de agosto de 2018 e, com entrada em vigor em 18 de setembro de 2020. Ainda que com o Marco Civil da Internet e a Lei Geral de Proteção de Dados (LGPD) tendo sido aprovados, a centralidade alcançada pelo debate da proteção de dados como garantia de outros direitos ainda permanece circunscrito em um campo de profissionais e especialistas das áreas do direito e da tecnologia.

O caráter tecnicista, tanto da legislação, quanto das tecnologias, faz com que essa discussão relevante e contemporânea permaneça afastada das populações mais vulneráveis às violações de direitos: pessoas racializadas como não-brancas, socioeconomicamente desfavorecidas e espacialmente confinadas em territórios periféricos, sem acesso à políticas públicas básicas. Apesar da tecnicidade inerente à questão, vê-se que a desproteção de dados se assenta em relações de poder que estruturam as relações sociais, raciais, políticas e econômicas.

Tendo como pano de fundo uma compreensão crítica como forma de dissecar relações de poder e proporcionar a transformação social, este capítulo objetiva cultivar saberes acerca da proteção de dados, especialmente pensando a GCD como ferramenta de participação social contra-hegemônica “na era dos dados”. Busca-se destacar a importância da participação cidadã, sobretudo por meio da metodologia da GCD harmonizada com a LGPD, para pessoas que integram Organizações do Terceiro Setor e movimentos sociais, na instauração de uma cultura de proteção de dados. Espera-se que este capítulo possa munir tais agentes e fazer florescer uma maior compreensão sobre o direito à proteção de dados e, enfim, contribuir para a garantia de outros direitos que interligam-se com esse.

O capítulo seguirá, portanto, a seguinte estrutura. Primeiramente, será realizada uma breve revisão de literatura a respeito da GCD, buscando construir um diálogo entre as compreensões e definições existentes em torno do conceito. O objetivo é dar insumos para a reflexão sobre como a GCD insere-se no debate de participação social e proteção de dados. Em seguida, traça-se uma análise do cenário de proteção de dados nacional, para se propor uma perspectiva de proteção dos dados. O objetivo do capítulo é construir uma leitura da GCD como ferramenta de fortalecimento de uma cultura de proteção de dados, a partir da sociedade civil, em especial das periferias.

## Parte 1.

# Entre Conceitos e Práticas: A Geração Cidadã de Dados e a Transformação Social nas e para as Periferias

---

Em junho de 2024, no 1º Encontro Nacional dos Observatórios de Saúde na Periferia, organizado pelo Ministério da Saúde, conversava com uma integrante de outra organização da sociedade civil, cujo principal objetivo é a produção de pesquisas e dados sobre e a partir do seu território. Essa organização é uma instituição parceira e que, anteriormente, já havia realizado atividades de colaboração e troca institucionais. Inclusive, em um intercâmbio entre nossas organizações, em 2022, apresentamos a metodologia de Geração Cidadã de Dados (GCD) como balizador do nosso trabalho no Instituto Decodifica (à época LabJaca) e foi reconhecido, por nós e por eles, à semelhança das nossas atuações nos nossos respectivos territórios. No entanto, em 2022, eles não utilizavam a nomenclatura “GCD”, talvez porque não conheciam o conceito. Em 2024, no nosso reencontro no evento de observatórios de saúde na periferia, eles continuavam não utilizando o nome GCD, nem se autodeclarando como uma organização de Geração Cidadã de Dados.

O episódio descrito acima não é um caso isolado. Muitas organizações Brasil afora, e provavelmente em todo o mundo, não conhecem o conceito da GCD, apesar de, na prática, operacionalizarem algo muito próximo a isso. Existem também aquelas instituições que, ainda que conheçam, optam por não utilizar o conceito. Obviamente, essa é uma prerrogativa e decisão que cabe a cada instituição, e que não está sendo questionada aqui. Contudo, enquanto membro da Rede GCD<sup>154</sup> e de uma organização que levanta a bandeira da Geração Cidadã de Dados, este quadro suscita alguns questionamentos: existe um entendimento comum ou basilar sobre a GCD? Qual o nível de compreensão compartilhado a respeito da GCD? Quais são os critérios mínimos para definir uma iniciativa como de GCD? Existem outras nomenclaturas utilizadas para práticas e metodologias participativas de levantamento de dados e de pesquisa? Se sim, a GCD se diferencia delas? Como? Finalmente, existe algum motivo para defender essa nomenclatura/conceito?

---

<sup>154</sup> “A Rede de Geração Cidadã de Dados foi criada por organizações que acreditam que esse tipo de tecnologia social é indispensável para a construção de uma democracia justa e plena no Brasil. A primeira semente para a formação da Rede foi plantada no I Seminário de Geração Cidadã de Dados que aconteceu nos dias 19 e 20 de setembro de 2023 na sede do data\_labe, no Complexo de Favelas da Maré, em parceria com a Casa Fluminense”. Acesse o manifesto da Rede GCD no link: <https://datalabe.org/manifesto-rede-gcd/>. Entre em contato pelo email: [geracaocidadadedados@gmail.com](mailto:geracaocidadadedados@gmail.com).



Os termos “Geração Cidadã de Dados” (GCD) ou “Dados Gerados por Cidadãos” (DCG) vem da expressão em inglês “*Citizen-Generated Data*” (CGD), o que revela, em primeiro lugar, que esta é uma nomenclatura de origem anglófona e, ainda que não se saiba precisamente sua origem, provavelmente trata-se do norte global. Apesar disso, ela é utilizada para descrever um fenômeno global e, conseqüentemente, diverso. Para além das especificidades que cada contexto nacional traria como desafio na construção de uma definição única destes termos, os nomes GCD/CGD também se propõem a englobar um conjunto muito grande de dados e/ou práticas de produção de dados. Tais como, *surveys* domiciliares, questionários individuais (online e offline), mapeamentos, entrevistas, grupos focais, entre outros. A isto, soma-se ainda o fato dos termos GCD e CGD englobarem práticas recentes e em constante transformação, visto que são afetadas por inovações tecnológicas e/ou metodológicas, cada vez mais recorrentes, como, por exemplo, o uso de *whatsapp* para entrevistas, mapeamentos, respostas de formulários etc. Este conjunto de fatores dá uma dimensão do desafio de construir uma definição de GCD/CGD que seja abrangente o suficiente para contemplar toda sua diversidade, mas também coerente e concreta o bastante para que existam fatores comuns palpáveis que deem algum sentido coletivo a esse conjunto.

Segundo Piovesan (2015), esse problema de definição da GCD e dos DCG afeta, de forma muito prática, a rotina e as possibilidades dessas iniciativas dialogarem com gestores públicos, órgãos governamentais e, com isso, conseguirem impactos de escala. A pesquisa realizada por Piovesan (2015) com funcionários do governo de 4 países (Argentina, Quênia, Nepal, Tanzânia) e com representantes de organizações internacionais, conclui que a falta de uma definição clara sobre a GCD/DCG e os diferentes significados que as expressões podem ter, para diferentes pessoas, são desafios cruciais que precisam ser vencidos. Não obstante, algumas iniciativas têm avançado nessa agenda.

A Civicus, uma rede internacional de organizações da sociedade civil, construiu sua definição de DGC, a qual é comumente citada pela literatura internacional sobre o tema<sup>155 156 157</sup>. Em sua frente de trabalho voltada para uso de DCG, o DataShift, eles definem:

---

<sup>155</sup> Jungcurt, S. Citizen-generated data: Data by people, for people. IISD, 2024. Disponível em: <<https://www.iisd.org/articles/insight/citizen-generated-data-people>>. Acesso em: 25/07/2024.

<sup>156</sup> PARIS21 & Philippine Statistics Authority. Use of Citizen-generated Data for SDG Reporting in the Philippines: A Case Study. PARIS21 Working Paper. 2020. Disponível em: <[https://paris21.org/sites/default/files/2021-02/CGD\\_FINAL\\_reduced.pdf](https://paris21.org/sites/default/files/2021-02/CGD_FINAL_reduced.pdf)>. Acesso em: 02/08/2024.

<sup>157</sup> TAP Network. Produzindo e apoiando dados gerados por cidadãos. In: SDG 16+ Civil Society Toolkit. [S. l.]: TAP Network, 2021. p. 3-13. Disponível em: <https://www.sdg16toolkit.org/explore/accountability-for-sdg16/producing-and-supporting-citizen-generated-data/>. Acesso em: 21/07/2024.

Dados gerados por cidadãos são informações produzidas por pessoas ou suas organizações para acompanhar, exigir ou impulsionar mudanças em questões que as afetam. Esses dados são fornecidos ativamente pelos cidadãos, oferecendo representações diretas de suas perspectivas e uma alternativa aos conjuntos de dados coletados por governos ou instituições internacionais”

(DATASHIFT, 2015, p. 1, tradução nossa)<sup>158</sup>.

A definição da Civicus/DataShift representa uma boa síntese dos elementos dos DGC. Ela identifica os atores envolvidos na sua produção - “pessoas ou suas organizações” -, indica seu propósito - “acompanhar, exigir ou impulsionar mudanças em questões que as afetam” - e marca o caráter crítico/alternativo dos dados produzidos, contrapondo-os àqueles coletados por governos e instituições internacionais.

Partindo de uma base comum à definição acima, Grageda, Schmidt e Ranjan<sup>159</sup> (2020) organizam sua explicação da GCD, estruturando-a em torno de três perguntas guias: “Quem faz?”, “Como se faz?” e “para que faz?”. Para esses autores, quem protagoniza a GCD/DGC são atores não-estatais. Eles reconhecem que esta definição inclui uma ampla gama de atores, no entanto, priorizam ressaltar, na sua definição, que os DGC são dados produzidos pelos seus usuários, ou seja, pelas pessoas ou grupos diretamente afetados. Já em relação à forma como esses dados são produzidos (“como se faz?”), a resposta é “com consentimento”. Os DGC devem ser fornecidos pelas pessoas de forma livre e, principalmente, conscientemente. Por último, em relação à finalidade ou ao “porquê”, o objetivo da produção de dados cidadãos é, segundo Grageda, Schmidt e Ranjan (2020), monitorar, demandar ou orientar questões que afetam os indivíduos ou suas comunidades. Neste sentido, sua definição de GCD está fortemente vinculada com participação e transformação social.

É importante destacar que a definição de Grageda, Schmidt e Ranjan (2020) propõe pensar, conjuntamente, esses três elementos: “quem faz”, “como faz” e “para que faz”. Sendo necessária a satisfação de todas as condições para identificação de um dado gerado de forma cidadã (*citizen-generated data*).

<sup>158</sup> The DataShift (2015). What is Citizen-Generated Data And What Is The DataShift Doing To Promote It? [Documento da Web]. Disponível em: [http://civicus.org/images/ER%20cgd\\_brief.pdf](http://civicus.org/images/ER%20cgd_brief.pdf). Acesso em: 23 de julho de 2024.

<sup>159</sup> Cázarez-Grageda, K., Schmidt, J. e Ranjan, R. (2020). Reusing citizen-generated data for official reporting: A quality framework for national statistical office-civil society organisation engagement. Paris21 Working Paper. Disponível em: [https://paris21.org/sites/default/files/2021-02/CGD\\_FINAL\\_reduced.pdf](https://paris21.org/sites/default/files/2021-02/CGD_FINAL_reduced.pdf). Acesso em: 05/07/2024.



As três definições detalhadas acima (DataShift, 2015; Piovesan, 2015; Grageda, Schmidt e Ranjan, 2020) contemplam concepções de diversas organizações internacionais tais como *Expert Group on Refugee, IDP and Statelessness Statistics* (EGRIS)<sup>160</sup>, Serviço de Estatística de Gana<sup>161</sup>, *Global Partnership for Sustainable Development Data*<sup>162</sup>, *World Vision*<sup>163</sup>, entre outras. Elas são definições que avançam na construção de critérios e elementos concretos, diferenciando-as de ideias genéricas, tais como a de Meijer e Potter (2018 apud CORCHO et al., 2022), segundo a qual os dados gerados de modo cidadão são “os dados que indivíduos conscientemente geram e que estão abertamente disponíveis para uso no domínio público”. Note-se, por exemplo, a ausência de intencionalidade dos dados nesta definição. Apesar disso, essas definições não esgotam as possibilidades de definição da GCD, nem solucionam algumas lacunas do conceito.

Em primeiro lugar, o critério de fornecimento voluntário e consciente pelos cidadãos, presente em Grageda, Schmidt e Ranjan (2020) fica fragilizado quando, na própria definição dos autores, dados obtidos por meio de pegada digital, ou seja, emails, dados de aplicativos, posts em blogs ou redes sociais e via cookies estão contemplados na sua definição. Esse aspecto do uso de dados de pegada digital como elemento “consciente” é altamente questionável, visto que, na maioria das vezes, embora dados de cookies e etc sejam consentidos pelos usuários, eles o são de forma quase inconsciente ou despolitizada. Aceitar o uso desses dados, obtidos de forma despolitizada, como DGC parece contra intuitivo em relação ao propósito de transformação social, ainda que não haja contradição conceitual nisso<sup>164</sup>.

A autoria da GDC e da GCD também é outro elemento que, analisando com maior profundidade os conceitos e observando a prática desses movimentos, cabem alguns questionamentos. Para Piovesan (2015) e DataShift (2015), a autoria dos DGC está relacionada a “pessoas e suas organizações”, ou seja, a

<sup>160</sup> Link: <<https://egrisstats.org/recommendations/other-recommendations/citizen-generated-data/>>.

<sup>161</sup> Statistical Service Ghana. Terms of Reference - Citizen Generated Data Gender-Based Violence Project. [S.l.]: Statistical Service Ghana, [S.d.]. Disponível em: <<https://statsghana.gov.gh/gssmain/storage/opportunity/Terms%20of%20Reference%20-%20GENDER%20.pdf>>. Acesso em: 17/07/2024..

<sup>162</sup> <https://www.data4sdgs.org/resources/advancing-sustainability-together-citizen-generated-data-and-sustainable-development>

<sup>163</sup> United Nations High Level Political Forum .Putting People at the Centre of the Data Revolution. 2019. Disponível em: <<https://sdgs.un.org/sites/default/files/2021-06/The%20Case%20for%20Citizen%20Generated%20Data%20for%20SDG%20Accountability%20final%20%281%29.pdf>>. Acesso em: 12/07/2024.

<sup>164</sup> É possível produzir transformação social, mobilizada por atores afetados pelo problema social em questão a partir de dados de pegada digital. Se isso ocorre, não há como negar o caráter cidadão desses dados, no entanto, chamar isso de Geração Cidadã de Dados, quando os dados foram produzidos sem essa intenção ou consciência, parece impreciso. Por isso, mais a diante será proposta uma diferenciação entre DGC e GCD.

sociedade civil. Nela, o mais vasto conjunto de atores estão potencialmente incluídos, ONGs, negócios de impacto social, *Think Tanks*, laboratórios de dados. Nessa definição, não há nenhuma condição quanto ao envolvimento dessas organizações e/ou pessoas com a temática.

Já no conceito trazido por Grageda, Schmidt e Ranjan (2020) produtores dos DGC são pessoas diretamente afetadas pela situação social sob análise. Isso representa um avanço, na nossa perspectiva, visto que atrela a produção de dados cidadãos a pessoas e grupos vinculados àquela realidade. Ainda assim, em algumas temáticas essa intenção de correlacionar a produção de dados cidadãos com as pessoas diretamente afetadas, pode ser diluída quando o problema social é mais difuso. Por exemplo, a segurança pública é uma temática de toda a sociedade, todas as classes e grupos sociais são afetados, ainda que em diferentes medidas, por ela. No entanto, sabe-se que populações racializadas, pobres e moradores de periferia são as mais vulnerabilizadas nesse quadro e as mais marginalizadas nos espaços de debate e decisão sobre o tema. Ter uma definição que assegure o protagonismo desses grupos na produção e uso de dados cidadãos seria um avanço político no debate.

Em última instância, talvez o grande desafio de definir os dados cidadãos e/ou a geração cidadã de dados está em conceituar não somente quem (como já exposto acima), mas principalmente, como se dá o protagonismo, os níveis de envolvimento e os papéis práticos na produção de DGC ou em projetos de GCD. Neste quesito, as definições apresentadas aqui são vagas em relação aos diferentes níveis de envolvimento cidadão e sua posição na cadeia de valor dos dados. Mesmo quando esses fatores são delimitados, entender como se dá esse envolvimento na prática é um grande desafio. Por exemplo, para Jungcurt (2022), com os DGC os indivíduos que se beneficiarão da coleta de dados estão diretamente envolvidos no design, coleta, análise e uso dos dados que os descrevem. Nesta definição, o papel dos cidadãos está em toda a cadeia de valor dos dados, o que representa um avanço na definição, mas o nível de ingerência e poder dos indivíduos beneficiados da coleta de dados não fica evidente nessa definição. Como é a relação entre esses indivíduos e o “corpo técnico” de pesquisa? Quem tem a palavra final nos processos?

Um esforço em escala global que tem chamado a atenção na tentativa de organizar um conceito amplo o suficiente, para abarcar diferentes possibilidades, mas uníssono o coeso o suficiente para propor uma unidade em meio a essa diversidade de compreensões dos DGC é a colaborativa global da ONU sobre Dados Cidadãos<sup>165</sup>.

Atentos à crescente relevância dos dados produzidos por cidadãos para o monitoramento dos Objetivos de Desenvolvimento Sustentável (ODS) em complementação aos órgãos governamentais de estatística, a ONU estabeleceu, em 2023, a “Colaborativa sobre os Dados Cidadãos (*Collaborative on Citizen Data*)”, no 4<sup>a</sup> Fórum Mundial de Dados, na China. Em setembro do mesmo ano,

<sup>165</sup> UNSD. Disponível em: <<https://unstats.un.org/UNSDWebsite/citizen-data/>>.



a Colaborativa encontrou-se em Copenhague na convenção intitulada “*The Copenhagen Framework on Citizen Data*”<sup>166</sup>. O objetivo da Convenção Quadro de Copenhague sobre Dados Cidadãos foi apresentar um quadro conceitual que avançasse na definição dos DGC e oferecesse uma compreensão comum dos conceitos relevantes<sup>167</sup>. Para isso, a iniciativa colaborativa sobre dados cidadãos abriu uma chamada global de contribuições sobre o tema, com objetivo de que atores da sociedade civil cooperassem com insumos para a construção dessa base conceitual.

Nessa iniciativa, os dados cidadãos foram definidos como “dados originários de iniciativas onde os cidadãos **iniciam** ou estão **suficientemente envolvidos**, no mínimo, nas **etapas de design e/ou coleta da cadeia de valor dos dados**, independentemente de esses dados serem integrados às estatísticas oficiais” (UN Statistics Division, 2024, p. 5, tradução nossa). Desta definição, são destacadas três características definidoras dos “dados cidadãos”: (1) o nível de participação social, (2) a etapa na cadeia de valor dos dados em que os cidadãos estão envolvidos e (3) o tipo de iniciativa para coleta de dados.

A participação social pode assumir diferentes níveis na produção de dados, desde o nível em que cidadãos, comunidades e ONGs se envolvem na produção de dados por iniciativa própria, com controle total do processo, até o nível em que a “participação social” é usada como tokenismo (UN Statistics Division, 2024). A iniciativa da ONU divide a participação social em 5 níveis: (1) informativa, (2) consultiva, (3) conciliatória (participação limitada), (4) parceria e (5) autodeterminação de cidadãos/comunidades (Arnstein, 1969 apud UN Statistics Division, 2024). Sendo que destes, apenas dados gerados com níveis 4 e 5 de participação são considerados como dados cidadãos. Enquanto a autodeterminação (5) descreve projetos criados que emanam diretamente das pessoas afetadas na produção dos dados, o nível 4 (“parceria”) estabelece que as tomadas de decisão na produção de dados cidadãos serão negociadas entre cidadãos, organizações da sociedade civil de apoio e funcionários públicos, com responsabilidades compartilhadas (UN Statistics Division, 2024).

Em relação à etapa em que deve se dar essa participação, a definição determina que seja: (1) na fase de *design*, onde os objetivos, parcerias, metodologias, abordagens para coleta de dados, bem como acesso, uso e aplicação dos dados são determinados; ou (2) na fase de coleta de dados. Embora não incluída na definição, destaca-se a relevância do engajamento cidadão em outras etapas da cadeia de valor dos dados, particularmente na adoção e uso dos dados.

Por fim, os tipos de engajamento cidadão/cívico são: (1) ação cívica, quando é totalmente impulsionada, gerada e pertencente aos cidadãos/comunidades/sociedade civil; (2) colaboração cívica, onde a iniciativa é da sociedade, mas

<sup>166</sup> <<https://egrisstats.org/recommendations/other-recommendations/citizen-generated-data/>>.

<sup>167</sup> UN Statistics Division. The Copenhagen Framework on Citizen Data. [S. l.], 2024. 34 p. Disponível em: <<https://unstats.un.org/UNSDWebsite/events-details/un55sc-copenhagen-framework-on-citizen-data-and-its-implementation/>>. Acessado: 01/08/2024.

é implementada em colaboração com o órgãos de estatística governamentais (NSOs) ou outros atores governamentais; (3) colaboração conjunta, na qual cidadãos e atores governamentais “co-criam” uma iniciativa de dados; (4) colaboração impulsionada pelo setor público, quando é iniciada por NSOs e implementada em colaboração com cidadãos/CSOs; (5) colaboração impulsionada por outros atores, onde outros atores iniciam o projeto e a implementação é feita em colaboração com cidadãos/CSOs; e (6) iniciativas de outros atores sem colaboração, a qual acontece sem colaboração com os cidadãos ou com engajamento limitado.

O quadro de Copenhagen sugere, portanto, uma taxonomia de classificação de dados cidadãos a partir de uma combinação dos três fatores acima: nível de participação social, etapa da cadeia de valor em que a participação social ocorre e a natureza do engajamento cívico/cidadão. Produções de dados no modelo de ação, cívica, colaboração cívica e colaboração conjunta dão origem a dados cidadãos (UN Statistics Division, 2024). Já dados advindos de colaboração impulsionada pelo setor público ou por outros atores, o nível de participação nas etapas de design deve ser de parceria e, na coleta de dados, deve ter envolvimento cidadão exceto em casos de ciência cidadã, onde essa fase pode ser delegada a outros atores.

A iniciativa da ONU lança um olhar complexo e multifacetado sobre dados cidadãos, representando um grande esforço em conceitualizar esses dados. Nesse caminho, a iniciativa acaba aprofundando-se em elementos da(s) forma(s) como os dados cidadãos são produzidos para poder identificá-los como tal e, com isso, é possível um olhar mais atento não somente para os Dados Cidadãos (DGC), mas também para a Geração Cidadã de Dados (GCD).

Dito isto, cabe buscar uma diferença de perspectiva que diferencie DGC e GCD. “*Citizen-Generated Data*” (CGD) pode ser traduzido de muitas formas: “geração cidadã de dados”, “produção cidadã de dados”, “dados gerador de forma cidadã”, “dados gerados por cidadãos”, entre outras. Enquanto em inglês, todas essas traduções e seus sentidos cabem no termo “*citizen-generated data*”, em português as sutis modificações das traduções supracitadas transformam-se em significativas diferenças de compreensão.

A tradução “dados gerados/produzidos por cidadãos” (DGC) traz foco ao produto/objeto (dados) e seu agente produtor (os cidadãos). Já o termo “Geração/Produção Cidadã de Dados” destaca a ação (geração/produção) e sua característica (cidadão). Assim, uma tradução (dados gerados por cidadãos) ressalta o objeto, uma categoria específica de dados, a saber, aqueles produzidos pelos cidadãos. Já a outra (produção cidadã de dados) destaca uma forma de ação, uma prática.

As definições apresentadas até o momento tratam na perspectiva dos dados gerados por cidadãos (DGC) ou dados cidadãos, suas definições tangenciam, em diferentes níveis, aspectos da forma como esses dados são produzidos. O quadro de Copenhagen é o que mais se aprofunda nesses aspectos, ainda assim, seu foco é sobre o objeto “dados cidadãos”.



Nossa proposta é abordar a GCD como prática, como metodologia e não como um tipo de dados. Existem os dados cidadãos, mas mais fundamental do que isso é olhar para a prática de produção cidadã de dados. Dados cidadãos podem ser gerados sem o protagonismo das pessoas diretamente afetadas por um problema ou ainda, podem ser gerados a partir de produtores tradicionais de conhecimento. Eles podem manter relações hierárquicas entre pesquisador e objeto. Eles podem hierarquizar saberes e podem, inclusive, delegar a participação social apenas à função de coleta de dados, inclusive por motivos pragmáticos.

A Geração Cidadã de Dados (GCD) observada como metodologia é uma prática política, é um mecanismo de participação social é uma ferramenta contra hegemônica de produção de dados e narrativas por e para as pessoas, grupos, comunidades e territórios mais vulnerabilizados. Nessa perspectiva, a GCD é uma prática de resistência, é um ato político, que faz uso dos dados para produzir um mundo mais justo. Obviamente que todos os conceitos construídos sobre dados cidadãos nos ajudam a entender o que é essa produção cidadã de dados. No entanto, nenhuma dessas definições destaca com clareza e completude o significado e o processo político quando se faz produção de dados em uma perspectiva periférica. Talvez a chave teórica que mais se aproxime dessa abordagem é o estatativismo (statactivism) da sociologia da quantificação. Contudo, ainda parece uma literatura demasiadamente acadêmica, fora do ciclo dos movimentos sociais e bastante europeia.

Uma abordagem da GCD que se destaca pelo olhar desse conceito como prática é o manifesto da Rede GCD, segundo o qual:

**A Geração Cidadã de Dados - GCD - compreende um conjunto de metodologias concebidas ou adaptadas pela sociedade civil para retratar, analisar e avaliar questões de interesse público, valendo-se de dados para a identificação de problemas e/ou potencialidades. Este processo envolve o engajamento da sociedade civil em todas as fases, desde a coleta até a distribuição dos dados, respeitando e recorrendo a conhecimentos, tecnologias e tradições territoriais e populares**

(MANIFESTO GERAÇÃO CIDADÃ DE DADOS, 2024, p.2).

O manifesto segue indicando alguns pressupostos do GCD, dentre os quais, vale destacar o primeiro, “Protagonismo de periferias, populações marginalizadas e sub-representadas no debate público e científico”. Esse pressuposto, em conjunto com a ideia do engajamento desses atores em todas as fases da cadeia de valor dos dados, confere a marca do protagonismo periférico nesse conjunto de metodologias e sua atuação em consonância com os conhecimentos, tecnologias e tradições territoriais e populares.

Esta é uma declaração metodológica, mas, sobretudo, política da abordagem que a Rede GCD possui em relação aos dados e sua produção. A rede, assim como o movimento da GCD no Brasil, é recente e ainda precisa ter seus conceitos e metodologias testadas na prática. Lidar com as dificuldades da sociedade civil brasileira, com o cenário de produção de dados no país e com a diversidade de instituições que compõem a rede, será um desafio a ser enfrentado pelo coletivo. No entanto, sua formação contribui para o olhar engajado dos dados, com protagonismo periférico, buscando fortalecer o movimento de GCD no Brasil, como prática de participação social.

Como prática política, a GCD possui também princípios. Entre os quais deve-se destacar para os objetivos deste capítulo, a proteção e segurança dos dados coletados e resultados obtidos. Enquanto ato político contra hegemônico, prática participativa e de protagonismo periférico, a GCD deve ter uma preocupação especial com a proteção de dados, visto que produz dados a partir e sobre periferias. Portanto, não tratar com seriedade e rigor a coleta, armazenamento, veiculação e proteção desses dados é vulnerabilizar, novamente, os grupos com os quais trabalha. Sobretudo quando compreende-se que esses são os grupos criminalizados, controlados, vigiados e marginalizados pela iniciativa privada e pelo Estado. Desse modo, por propor-se como mecanismo de participação e transformação social para esses grupos, a GCD não pode, ainda que não-intencionalmente, colocar em risco da segurança digital de indivíduos ou organizações periféricas. Contrariamente, a GCD deve ser um movimento que lidera a construção de uma cultura de proteção dos dados e deve ser também um movimento de conscientização, se possível, fiscalização e melhor ainda de implementação de segurança de dados de pessoas, comunidades e grupos periféricos.

Vale notificar, em suma, que o presente tópico destaca o papel fundamental da participação cidadã na produção de dados, que são utilizados como ferramentas para a transformação social na busca pela garantia dos direitos que não são usufruídos em sua plenitude, especialmente em contextos de marginalização e desigualdade. Portanto, advém desses fatores a importância de definir e aplicar metodologias de Geração Cidadã de Dados (GCD) para dar voz aos territórios periféricos e garantir que os dados gerados reflitam suas realidades. Nos tópicos a seguir, se buscará ampliar essa discussão, destacando-se a necessidade de uma cultura de proteção de dados para garantir a participação cidadã robusta. Isso, enfatizando-se ainda que a proteção de dados é essencial para participação ativa e consciente dos cidadãos é essencial; não apenas para a criação de dados significativos, mas também para a construção de uma sociedade que respeite e promova os direitos de todos, especialmente daqueles que mais necessitam de visibilidade e proteção, sobretudo nesta também chamada Era da Informação.



## Parte 1.2

### Proteção de Dados e Cidadania: Construindo uma Narrativa Inclusiva através da análise ao atual cenário social

É cediço que os assuntos relacionados à Proteção de Dados têm tomado proporções imensas, seja no Brasil ou mundo afora, em nosso contexto atual. Não por outro motivo, essa se tornou uma das maiores discussões no meio jurídico-acadêmico, em uma evidente tentativa de entender as dinâmicas impostas dentro de um universo globalizado e cada vez mais tecnológico que desafia os limites éticos e legais existentes, no que se refere a massiva circulação de dados.

Conforme contextualizamos no capítulo “Justiça Racial e Proteção de Dados”, as tecnologias estão cada vez mais ligadas ao nosso convívio social, fazendo parte inclusive de políticas públicas de Estados e governos – seja no setor da educação, transporte público ou mesmo dentro da segurança pública. Embora essas tecnologias possam parecer, à primeira vista, um “avanço”, é necessário analisar de forma crítica os seus verdadeiros impactos, sobretudo levando em consideração quais são os locais em que esse aparato tecnológico é empregado, e quem são as pessoas afetadas.

Nesse aspecto, faz-se essencial pensarmos, ainda, quem produz os códigos e métricas das tecnologias ora empregadas. Na prática, todavia, observamos que as tecnologias utilizadas em tais políticas, como as de reconhecimento facial, por exemplo, trazem com si vieses e contextos de discriminação<sup>168</sup>, fato que influi diretamente na interpretação dos dados obtidos de raça, gênero e etnia, promovendo assim uma automatização de opressões históricas, além de potencializar exponencialmente o seu uso por governos mais conservadores em um cenário de extrema vigilância, ocasionando a diminuição da liberdade e da privacidade das pessoas afetadas.

Os dados pessoais utilizados como matéria prima e/ou resultado das tecnologias na (re)construção de uma política pública não são informações “frias” ou um mero aspecto sobre determinada pessoa. Eles guardam diferentes histórias e vidas, sem mencionar traços drásticos de processos históricos (a exemplo dos quase quatrocentos anos de escravidão aos quais atravessou o território brasileiro, que ainda convive com fortes resquícios do período) que são ignorados

---

<sup>168</sup> A exemplo da vivência experienciada por Joy Buolamwini, aluna negra do MIT (*Massachusetts Institute of Technology*), em cenário no qual estava trabalhando com um *software* de análise facial quando percebeu que o mesmo não detectou seu rosto, depreendendo a partir desse episódio que, os indivíduos que codificaram e instituíram as métricas do algoritmo não o ensinaram a identificar uma ampla gama de tons de pele e estruturas faciais, sobretudo de pessoas negras. BUOLAMWINI, Joy. **How I'm fighting bias in algorithms**. TEDxBeaconStreet. Nov 2016. Disponível em: <[https://www.ted.com/talks/joy\\_buolamwini\\_how\\_i\\_m\\_fighting\\_bias\\_in\\_algorithms](https://www.ted.com/talks/joy_buolamwini_how_i_m_fighting_bias_in_algorithms)> Acesso em julho de 2024.

no momento de formulação das citadas políticas públicas, potencializando ainda mais as desigualdades já enfrentadas por tais grupos. Sendo assim, é necessário avaliar a finalidade/necessidade do uso de um dado pessoal, que pode vir a se tornar um dado pessoal sensível, quando ele se mostrar potencialmente discriminatório, podendo promover ainda mais injustiça.

Nesse aspecto, surge ainda a Lei Geral de Proteção de Dados, que foi aprovada no ano de 2018, na forma da Lei nº 13.709, de 14 de agosto de 2018 e, com entrada em vigor em 18 de setembro de 2020. A normativa surge em um cenário no qual se busca definir diretrizes para a consolidação da regulação de um ecossistema de proteção dos direitos à privacidade e de dados pessoais. A referida lei visa também, dentre outros objetivos, (i) garantir a igualdade material e a liberdade das pessoas naturais; (ii) assegurar o livre desenvolvimento da personalidade do ser humano; (iii) impedir discriminações ilícitas e/ou abusivas; (iv) evitar que determinados grupos sofram restrições indevidas a bens e cenários de preconceito e estigmatização.

Todavia, a linguagem tão tecnicista e pouco acessível das discussões acerca das finalidades protetivas da referida lei faz com que essas não cheguem a toda a população de modo uniforme, afetando sobretudo as populações mais vulnerabilizadas, tais quais as de favelas e periferias. Isso já traz, por si só, um prejuízo inimaginável e incalculável às mesmas, o que as torna reféns da falta de informação e/ou da inacessibilidade da informação veiculada. Este fato, isoladamente ou não, retira ainda mais a possibilidade de um debate democrático em face desse assunto extremamente caro, justamente por se referir à autonomia individual. Isso sem mencionar ainda o impacto negativo sobre a própria eficiência prática e material dos direitos que a LGPD visa garantir.

Ponto que contribui para corroborar com tal narrativa, é o fato de que, segundo o Instituto Brasileiro de Geografia e Estatística (IBGE), a população negra é composta por 55,8% da população, sendo, portanto, a maioria absoluta. Todavia, se analisarmos a taxa de analfabetismo da mesma, esta se verifica como quase o dobro, se comparada com a população branca, correspondendo a um número de 20,7% da população<sup>169</sup>. Isso, ao passo que acaba sendo sub-representada politicamente, com uma população de 8,8% de prefeitos e vereadores eleitos (com base nos dados coletados no ano de 2020), em detrimento, assim sendo, da sobrerrepresentação da população branca - “60% a mais de prefeitos brancos eleitos do que pessoas brancas na população e também cerca de 30% de vereadores brancos a mais”<sup>170</sup>.

<sup>169</sup> Cf. IBGE – Instituto Brasileiro de Geografia e Estatística, 2019 (Primeira Edição). **Desigualdades sociais por cor ou raça no Brasil**. Disponível em: <[https://biblioteca.ibge.gov.br/visualizacao/livros/liv101681\\_informativo.pdf](https://biblioteca.ibge.gov.br/visualizacao/livros/liv101681_informativo.pdf)> Acesso em julho de 2024.

<sup>170</sup> Cf. IBGE – Instituto Brasileiro de Geografia e Estatística, 2022 (Segunda Edição). **Desigualdades sociais por cor ou raça no Brasil**. Disponível em: <[https://biblioteca.ibge.gov.br/visualizacao/livros/liv101972\\_informativo.pdf](https://biblioteca.ibge.gov.br/visualizacao/livros/liv101972_informativo.pdf)>. Acesso em julho de 2024.



A discussão extremamente excludente da temática de proteção de dados impede a formulação de políticas para todos. Na verdade, formulam-se políticas para “os outros” (dentro de uma perspectiva de verticalidade da formulação e monitoramento de tais políticas, em detrimento da horizontalidade), retirando-se um aspecto fundamental de cidadania das populações mais vulnerabilizadas. É preciso repensar essa lógica sob a perspectiva de um pensamento humanizado, de modo a trazer essas pessoas para o debate. E não só isso, como garantir também que possam ter um posicionamento ativo, autônomo, e elucidado sobre o assunto, garantindo o acesso à informação e amplificando suas vozes – fugindo da falácia existente de que todos conhecem e falam sobre essa temática.

A exemplo, cita-se a possibilidade tanto do poder público quanto do privado incentivarem a promoção oficinas, rodas de conversa, palestras e eventos que apresentam a temática da proteção de dados, políticas desenvolvidas com fulcro nela, às pessoas, incitando aos debates, além de um momento de compartilhamento de experiências acerca de tais atores a um nível local, regional e nacional<sup>171</sup>. Tal medida potencializa a apropriação desse tema a tal população, além de empoderá-la, podendo ainda amplificar sua voz.

Para que haja uma efetiva proteção de dados, vale pensar numa perspectiva mais prática da participação cidadã, em uma ótica na qual se possa co-construir, ou seja, não apenas construir em relação ao outro, devemos nos colocar como parte do problema para gerar uma solução efetiva, dentro da realidade da conexão direta com os anseios de políticas sociais mais latentes. Nesse sentido, vale ter em mente que a citada participação cidadã – **na forma da metodologia GCD** – traz com si a ideia de que os territórios periféricos têm conhecimento empírico acerca da realidade que vivenciam, ainda mais se tratando do processo de formulação, monitoramento da execução e avaliação de uma política pública. Inclusive, esse elemento de participação é que tem o potencial de conferir cidadania de modo mais concreto, garantindo o protagonismo a um grupo sub-representado dentro do modelo democrático ao qual estamos inseridos.

Cabe considerar neste universo a promoção da cultura da informação e conhecimento, sobretudo quanto ao direito fundamental ao qual a Lei Geral de Proteção de Dados visa proteger: a privacidade e a autonomia privada<sup>172</sup>. Atuando dessa forma, estaremos contemplando as pessoas vulnerabilizadas sobre quem estamos produzindo nossas pesquisas e políticas, vez que somos parte, em alguma medida, dessa população.

---

<sup>171</sup> ROCHA, Viviane Helena da; NASCIMENTO, Thiago; SOUSA, Bruno. Favela também desenha, monitora e avalia política pública. Nexo Jornal. Disponível em: <<https://pp.nexojornal.com.br/opiniao/2023/03/13/favela-tambem-desenha-monitora-e-avalia-politica-publica>>. Acesso em julho de 2024.

<sup>172</sup> MULHOLLAND, Caitlin Sampaio. **Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18)**: Faculdade de Direito de Vitória (FDV). Revista de Direitos e Garantias Fundamentais, Vitória, ES, v. 19, n. 3, p. 159-180, set./dez. 2018. Disponível em: <<https://bdjur.stj.jus.br/jspui/handle/2011/179531>>. Acesso em julho de 2024.

A partir da concepção da construção horizontal das medidas que visam a real proteção de dados, em co-construção, vale também pensar acerca da ausência de diversidade no que tange a composição que abrange os tomadores de decisão, perpassando por setores desde os governos até as instituições da sociedade civil e empresas<sup>173</sup>. Tal quesito é fundamental para que se possa construir uma cultura que promova um maior diálogo entre diferentes grupos sociais e suas múltiplas facetas, principalmente para se ter um olhar de fato humanizado para as populações mais vulnerabilizadas, igualmente titulares de dados.

O quesito da diversidade vai ao encontro do princípio fundamental da igualdade, principalmente a material, preconizado pela Constituição Federal de 1988 - em seu art. 5º<sup>174</sup> - a qual advoga também pela busca do equilíbrio de representação em um sistema que se mostra tão heterogêneo, em contraponto à homogeneidade corporativa. A diversidade na tomada de decisões emerge, diante disso, como um componente essencial na edificação de um ambiente verdadeiramente democrático e igualitário, além de de fato representativo.

## Parte 1.3

### Garantindo Direitos e Humanizando Dados: Cultivando uma Cultura de Responsabilidade Social

A partir do debate proposto no que concerne à responsabilidade social para com os particulares tanto de Movimentos quanto de Instituições do Terceiro Setor perante as desigualdades dos importantes indicadores sociais abordados, vale aqui a singela tentativa de se criar uma **cultura** que poderá ser incorporada como uma guia com o condão de buscar garantir o menor potencial de dano possível para que tais entes, para que, ao produzirem suas pesquisas, não infrinjam os direitos que a LGPD visa garantir. Vale dizer que, diante da lógica abordada referente aos objetivos que tais entidades possuem em face das populações historicamente vulnerabilizadas, não há negociação entre garantir certos direitos em detrimento de outros. Neste ponto, considera-se a integralidade de direitos desses cidadãos.

Em que pese a citação de Instituições do Terceiro Setor que sejam de pesquisa, levando-se em conta a base legal do art. 11, II, alínea “c” da LGPD, que autoriza o tratamento de dados, mesmo que não seja verificado o requisito do

<sup>173</sup> A despeito disso, cita-se novamente a pesquisa Desigualdades sociais por cor ou raça no Brasil, realizada pelo IBGE, a qual identificou que 69% dos cargos gerenciais no país são ocupados por pessoas brancas, enquanto que apenas 29,5% são ocupados por pessoas pretas ou pardas. Cf. IBGE – Instituto Brasileiro de Geografia e Estatística, 2022 (Segunda Edição). Desigualdades sociais por cor ou raça no Brasil. Disponível em: <[https://biblioteca.ibge.gov.br/visualizacao/livros/liv101972\\_informativo.pdf](https://biblioteca.ibge.gov.br/visualizacao/livros/liv101972_informativo.pdf)>. Acesso em julho de 2024.

<sup>174</sup> Art. 5º. “Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à **igualdade**, à segurança e à propriedade, nos termos seguintes:”.



consentimento da pessoa titular, este ponto deve ser subjetivamente levado em conta por tais organismos. Sempre que possível, é fundamental **considerar a pessoa de quem aquele dado irá traduzir uma informação**, humanizando assim a própria relação que estará ali sendo construída, oferecendo-lhe a oportunidade de ter uma manifestação livre, informada e inequívoca pela qual concorda com o tratamento de seus dados pessoais para uma finalidade determinada (art. 5, XII, LGPD).

Ademais, mesmo que a própria Lei nº13.709, de 14 de agosto de 2018, forneça mandamentos para um maior rigor para o tratamento de dados e a implementação de medidas técnicas de segurança especializada (o que é extremamente válido, sobretudo pensando em organizações já minimamente estruturadas), é necessário considerar a proteção dos dados, sejam eles pessoais ou sensíveis, de como a **considerar o contexto em que se está**, considerando não só no tempo e no espaço, mas de acordo também com o grau de estrutura e complexidade da organização. Seja ela de menor ou maior grau, não necessariamente tem que proteger os dados, mas sim as pessoas.

Cabe, ao pensar nessa cultura ser instaurada, a **real necessidade** de se solicitar um dado. Se não há de fato uma necessidade claramente definida para que seja solicitado esse dado, ele não deve ser pedido. O pensamento é análogo quanto à questão de sua **finalidade**. Nesse quesito, ressalta a professora Caitlin Sampaio Mulholland: “Pelo princípio da finalidade, os dados devem ser tratados para determinados propósitos, que devem ser informados ao titular de dados previamente, de maneira explícita e sem que seja possível a sua utilização posterior para outra aplicação.”<sup>175</sup> ).

Ainda nessa perspectiva de se pensar os direitos fundamentais, é válido **verificar a hipersensibilidade dos dados dos hipervulneráveis** – ideia de tratar os iguais como tais e os desiguais na medida de sua desigualdade, tais como os grupos de crianças e adolescentes, ou de idosos, pessoais com deficiência, por exemplo, fazendo-se alusão ainda ao princípio da não-discriminação, tutelado sobretudo pela Carta Maior, bem como pela própria LGPD, pelo qual se depreende que, fica vedada a utilização dos dados pessoais para fins discriminatórios ilícitos ou abusivos.<sup>176</sup>

A **transparência**, nessa esteira, torna-se também elemento imprescindível, essencial para balizar as ações de entes como Movimentos Sociais e/ou Organizações do Terceiro Setor que utilizam a metodologia GCD, que veem na produção de dados, uma possibilidade de transformação social, seja por meio de políticas públicas ou ações locais eficientes com base neles, pois oferece

<sup>175</sup> MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18): Faculdade de Direito de Vitória (FDV). Revista de Direitos e Garantias Fundamentais, Vitória, ES, v. 19, n. 3, p. 159-180, set./dez. 2018. Disponível em: <<https://bdjur.stj.jus.br/jspui/handle/2011/179531>>. Acesso em julho de 2024.

<sup>176</sup> Ibidem.

lisura à tal atuação. Tal quesito demonstra a possibilidade de retificação da pessoa titular (sendo importante a anonimização ou pseudo anonimização de dados que se revelem sensíveis e com potencial discriminatório), além de informar a própria sociedade no que tange a informação veiculada. Ainda, pode ser vista como elemento fundamental para a manutenção da democracia.

Este conjunto de práticas principiológicas foi pensado para conferir humanidade aos processos de produção de dados pessoais e dados pessoais sensíveis, que visam especialmente construir uma cultura na qual se possa garantir efetiva proteção não só dos dados, mas das pessoas às quais eles estejam se referindo. É relevante enfatizar novamente a importância deles não só para o novo modelo de produção no contexto de espaço-tempo que estamos inseridos, mas para que se tenha um engajamento cívico ainda mais efetivo por aqueles que fazem parte dos territórios.

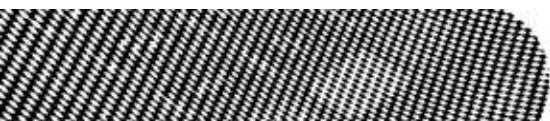
A promoção de uma cultura de responsabilidade social e de proteção de dados, por meio da atuação de Organizações do Terceiro Setor, aliados à participação cidadã, é essencial para assegurar os direitos fundamentais aos quais a LGPD visa proteger, sem comprometer a integralidade dos direitos dos cidadãos. A transparência, a participação cidadã e a consideração da diversidade tornam-se elementos-chave nesse processo, objetivando-se construir uma sociedade mais justa e inclusiva.

O conjunto de práticas principiológicas anunciado, sendo este baseado nos conceitos e princípios da manifestação livre, informada e inequívoca, com a contextualização no espaço-tempo e estrutura do grau de complexidade da Organização, e em suas respectivas suas necessidades em solicitar um dado para produzir uma pesquisa pensando em políticas públicas, bem como na finalidade, considerando a hipersensibilidade dos dados dos hipervulneráveis, fundados no princípio de transparência para tais ações, potencializam o fortalecimento da instauração de uma cultura efetiva de proteção de dados. Mais do que os dados, em si, deve-se buscar proteger as pessoas de quem as informações estão se referindo.

# SOBERANIA DE DADOS

Polinho Mota





## POLINHO MOTA

É nascido e criado em Manaus, atualmente mora no Rio de Janeiro onde atua como coordenador de dados e DPO do data\_labe, laboratório de dados com foco em gênero, raça e território.

Possui mestrado e atualmente está no doutorado em Epidemiologia e ciência de dados populacionais na UFRJ. Polinho acredita e trabalha para a democratização das tecnologias, feitas por todas as pessoas de forma livre e soberana.



# Soberania de dados

Desde 2020 eu comecei a participar de eventos e discussões que envolvem o mundo digital como membro da sociedade civil organizada, graças à função que desempenho no [data\\_labe](#). Antes disso, eu já havia concluído o meu mestrado e para a minha surpresa, pude comprovar que as visões sobre soberania de dados são bem distintas e até mesmo opostas a depender do programa de pesquisa e organização da sociedade civil que conheci. Logo no começo desse processo eu tinha tido pouca ou nenhuma formação do que é sociedade civil de fato, menos ainda, sobre o que significava soberania de dados, e acredito que pela minha breve e intensa experiência, a maioria de nós envolvidos nesses campos têm um padrão bem parecido com o meu. A gente entra num campo de pesquisa ou na sociedade civil sem saber direito as regras, os limites e as definições, porém conforme a bola vai rolando, as faltas vão sendo cometidas, (consequentemente os cartões e expulsões) a gente vai aprendendo e contornando conceitos muito difíceis de serem transformados em palavras que façam sentido pra gente e pra quem está lendo a gente.

Portanto, acreditem, eu estou plenamente consciente que tenho uma missão muito difícil a ser cumprida neste capítulo, primeiro porque nem mesmo nas discussões que envolvem o Governo, a iniciativa privada, a universidade e a sociedade civil, o termo “soberania de dados” possui um limite ou uma definição aceita por todos esses setores. Sempre que eu tenho um desafio muito grande como esse, eu olho para ele como aprendi tudo o que sei sobre o candomblé. É preciso viver, estar, sentir e gastar muitas horas ouvindo e vendo pessoas mais antigas desempenharem funções com muita naturalidade e destreza. Depois de um tempo eu começo o processo de imitação daquilo que vi, porém rapidamente a minha própria essência começa a ser impregnada nos meus movimentos e crio uma forma que é ancestral, mas muito minha. De vez em quando alguém mais velho olha e me dá um grande coió (briga ou alerta na gíria carioca), ou Deus me livre, minha Mãe de Santo me diz que está tudo errado e preciso perguntar “por que não pode ser assim?” ou ainda, “por que não pode ser feito desse novo jeito?”. Quando isso ocorre, o sentimento de vergonha invade o meu corpo por inteiro, porque me sinto desrespeitando séculos de tradição e me sinto como um menino teimoso que sempre quer fazer as coisas do meu jeito. Porém, não raramente, sou pego por comentários orgulhosos dizendo “eu nunca pensei que dava pra fazer assim”, ou “nossa irmão, assim é mais fácil né?”, e aí meus olhos se enchem de lágrimas porque sei que não sou só eu, mas as forças ancestrais que carrego no meu sangue e cabeça que sempre se reinventam, com a força de um vulcão e com a profundidade muito intensa que só as terras muito profundas podem dar.

Então começo esse capítulo fazendo dois compromissos, terei o máximo respeito por todas as minhas companheiras e companheiros do campo, porém vocês vão sentir um toque muito pessoal de quem aprendeu a fazer tecnologia nas favelas e comunidades urbanas (que irei escrever aqui sempre

como periferia), e apontando as coisas que vi, vivi e propus como solução em conjunto com aqueles que todo dia constróem novas tecnologias à partir das periferias. Pra começo de conversa, te trago meu fio principal dessa grande tapeçaria que vamos costurar: **a nossa soberania sempre foi pra gente!** Meu segundo compromisso é que você vai terminar este capítulo com uma visão mais ampla, conceitos traçados e apontamentos de caminhos a seguir sobre soberania de dados. Como você em breve vai descobrir, soberania tem tudo a ver com o poder de se rebelar. Boa leitura!

## Vamo de trás pra frente?

No dia 17 de Maio de 2024 ocorreu uma reunião puxada pela nossa Agência Nacional de Telecomunicações (ANATEL) que de forma surpreendente votou por uma iniciativa que colabora para termos alguma soberania nacional digital e de dados. *Primeiro, vou te explicar direitinho o que aconteceu pra depois a gente chegar no que defendo como soberania de dados.* Essa reunião foi uma das atividades do GAPE, que é o Grupo de Acompanhamento do Custeio a Projetos de Conectividade de Escolas, que “tem como finalidade a consecução de projetos de conectividade de escolas públicas de educação básica”. Essas ações para levar Internet de qualidade para escolas em lugares remotos foi uma das promessas de campanha do Presidente Lula e que, posteriormente entrou em seu plano de Governo. Além disso, é também uma contrapartida do leilão do 5G que visa modificar a infraestrutura de conexão no Brasil para poder levar a velocidade do 5G para todo o país.

Porém, levar sinal de Internet a qualquer lugar sempre foi uma decisão política com disfarces de decisões simplesmente financeiras, conforme mostram Geisa Santos, Luis Gustavo e Thiane Neves no artigo sobre conectividade na Amazônia. Quando o nosso país começou a estruturar toda a malha de cabos e antenas para levar Internet para todo o país, escolheu-se por começar pela região Sudeste, para a surpresa de zero pessoas, e depois disso pouca coisa mudou. Esse processo, somado ao descaso de políticas públicas regionalizadas levou ao deserto de conectividade nas regiões Norte e Nordeste, que fica flagrante na Imagem 1 que mostra o mapa das fibras ópticas na América do Sul. Para tentar mitigar esse problema uma das soluções é a conexão via satélite, que independe de malha de cabos e antenas e facilita a recepção do sinal via antena, algo que Elon Musk se adiantou em lançar para o mundo com suas antenas de conexão da Starlink, como explicam melhor Jessica Botelho, Lori Regattieri e Thiane Neves. Então, na cabeça de muita gente parecia óbvio que o Governo, já que precisava levar Internet para escolas no Norte e Nordeste, pudesse comprar uma antena do Kiko dos Foguetes e botasse lá, pronto!

Mas é aí que um plano de soberania entra em jogo. Acontece que os **dados** de conexão da Starlink pertencem a uma empresa privada e ainda da gringa, o que faz com que toda a troca de informações fique armazenada e passível de ser acessada onde e quando eles quiserem. Além disso, todo o lucro dessas compras milionárias iria pros bolsos dos acionistas da Starlink e do próprio Elon Musk, aliás por que vocês acham que o antigo Ministro das Telecomunicações,

Fabio Faria, se reuniu (mais desdobramentos aqui) SEM AGENDA DE GOVERNO com o dito cujo?

Então vejam, o Brasil vai ter que investir no projeto de conectividade das escolas, mas ao invés de gastar esse dinheiro com uma empresa de fora do Brasil e não ter autonomia digital nenhuma sobre esses dados, no dia 17 de Maio a Anatel anunciou que vai investir na Telebrás para que ela desenvolva em nosso país tanto as antenas, como a chamada constelação dos satélites que enviam o sinal de baixa órbita. Isso fará com que o próprio Governo ganhe um retorno financeiro com essa compra, bem como estimulará a competição do mercado entrando como mais um ator que pode prover esse tipo de conexão. Além de tudo, fica mais fácil de fazer acordos, em casos de investigações criminais, como por exemplo do uso de antenas de Internet em terras de garimpo ilegal. Não é simples, mas nunca será, e decisões como essas colocam o nosso país em outro nível dessa discussão, evidentemente que precisamos ficar atento aos acordos que se darão, aos editais de contratação, ao cumprimento dos prazos estabelecidos, mas isso teria que ser feito com qualquer empresa. Investir na tecnologia e inovação nacional é fundamental para caminharmos para um horizonte de soberania de dados. Aonde poderíamos a qualquer momento decidir pela manutenção de um serviço, atualização do mesmo, ou quem sabe implementar inovações que consideramos estratégicas para o nosso benefício.

#### Imagem 1: Mapa de cabos de fibra ótica na América do Sul



Fonte: ITU (2023)

Essa ação direta do governo brasileiro em prover a conectividade com soluções nacionais é quase que o oposto do que defendia John Perry Barlow, na sua [declaração do ciberespaço](#). Vejam, por exemplo, apenas um trecho que o autor dirige aos governos da época: *“Eu declaro o espaço social global aquele que estamos construindo para ser naturalmente independente das tiranias que vocês tentam nos impor. Vocês não têm direito moral de nos impor regras, nem ao menos de possuir métodos de coação a que tenhamos real razão para temer”*. Barlow, defendia que todo o ciberespaço devesse existir sem interferência nenhuma dos governos, que isso prejudicaria a liberdade que a Internet do começo dos anos 90 tanto defendia. Certamente que o contexto é completamente diferente, mas o Brasil é reconhecido internacionalmente pelo seu modelo de governança multissetorial, que envolve o Governo, as universidades e pesquisas, a iniciativa privada e a sociedade civil. Graças a esse modelo que conseguimos avançar, às vezes, ou tensionar para que as decisões sobre a Internet, com grandes consequências no âmbito digital e dos nossos dados pessoais, levem em consideração a visão de diferentes atores. Vejam então, que soberania de dados nem sempre está relacionada à ideia de individualismo ou simplesmente de autonomia legislativa em um território nacional, mas sim com a ideia de respeito aos indivíduos envolvidos em todo o processo ou a cada projeto..

## Chegando lá atrás

Barlow defendia que os países deveriam deixar de importunar a Internet, ele era representante ou com ligações com o partido republicano dos Estados Unidos, o que já diz bastante dessa defesa neo liberal de isenção total do Estado, porém ele ajudou a criar a [Eletronic Frontier Foundation](#) que atua nos direitos na Internet, por isso até hoje é bastante defendido por ativistas do direito digital, tendo em vista que esse autor ajudou a fomentar o mito da independência da Internet. Ainda no começo das discussões sobre soberania temos ainda as contribuições de Jean Pauldin que criou o conceito de soberania, onde os governos teriam liberdade para fazerem suas políticas em seus territórios, porém essa ideia de soberania sofre muita influência do iluminismo e neoliberalismo. Existe ainda [Carl Schmitt](#), que declara que o Estado com soberania é aquele que tem poder de declarar o estado de exceção. Aqui eu preciso fazer um enorme alerta e incômodo sobre esses dois autores tão reconhecidos como teóricos sobre os conhecimentos do que se entende por soberania. Como já disse, Barlow tinha ligações profundas com o partido republicano norte americano e já Schmitt, enquanto vivo integrou o partido nazista da Alemanha por volta dos anos 30. Quando passei a estudar soberania, aquelas pessoas que estavam orientando as aulas e debates insistiam que devíamos separar os autores das obras e que de alguma forma seus construtos eram válidos para pensarmos as democracias ocidentais, quiçá globais.

Permitam-me ser **rebelde** e manter uma coerência a declarar que não. Não tenho como me apegar a autores que deliberadamente defendem ideias contra humanas e contra o meu povo. Para Schmitt o soberano em uma democracia é

aquele ator ou ente que decide quando, por exemplo, suspender a Constituição em casos de exceção, e com toda certeza, posteriormente, devolve ao Estado sua fase comum democrática que contém os aparatos jurídicos e legislativos suficientes para continuar com a democracia. Se eu quiser seguir o mesmo caminho proposto por esses famosos autores, eu estaria sendo subjugado a ideias de poder que tiraram de mim e do meu povo qualquer possibilidade de soberania ou de vida. Todo o ordenamento dito legal e democrático no Brasil foi construído sobre milhares de corpos negros e indígenas assassinados e massacrados para que se instaurasse um modelo de poder defendido como humano e consequentemente democrático. Então vejam, atualmente se entro em uma discussão sobre soberania ou se sou convidado a escrever um capítulo de um livro sobre o tema, é esperado de mim que eu desenvolva meu pensamento por conhecimentos e princípios democráticos que são sanguinários e de extermínio a tudo aquilo que não tem em seu fundamento a branquitude e a Europa.

Mas aqui lanço meu maior fundamento para soberania que é a **“opção de se rebelar”**. O Brasil nasceu e se desenvolveu como uma colônia, mesmo depois que nossa suposta independência foi declarada pelo filho do Imperador português, nada mudou nesse dito Brasil. Vejam se faz sentido também pra vocês. Os nossos povos indígenas estavam aqui, possuíam seus modelos de gestão e convivência estabelecidos pelos seus deuses e fundamentalmente pela natureza. Em 1500 d.C. chegaram os invasores portugueses que decidiram saquear todo recurso natural a que tivessem alcance, para isso, declararam que o nosso território era de Portugal. Para garantir que esse processo acontecesse, baseados na sua fé, decidiram que indígena tinha que virar católico e que quem era africano sequer tinha alma e, por isso, poderia servir de escravo para garantir que os portugueses enriquecessem à custa do nosso território e da mão de obra escrava. Aos indígenas e africanos não existia opção, era fazer o que português mandava ou era morto. Mas daí, não só um, mas milhares de indígenas e africanos decidem iniciar um processo soberano sobre seus corpos, suas crenças, suas vidas e decidem **AQUILOMBAR!**

Em nenhum momento, até onde sabemos, indígenas e africanos aquilombados tentaram negociar ou se adaptarem à visão portuguesa do que era possível para serem minimamente soberanos sobre si próprios. **Pois é impossível soberania mínima, soberania tutelada, soberania negociada com quem quer te matar.** Aquele grupo de pessoas olhou pra todo o sistema montado por Portugal e sem perguntar se podiam, ou como deveriam fazer, migraram para dentro da floresta e sertão brasileiro e fundaram seu próprio território. Dentro do Império, eles fundaram o seu Império. Com suas regras, seus conhecimentos e suas relações, os indígenas e africanos aquilombados decidem deixar os portugueses jogarem seu jogo, pois compreenderam que naquele jogo jamais poderiam entrar, ou muito menos vencer.

Como Clóvis Moura argumenta em sua obra Rebeliões da Senzala, os escravizados na época tomam a decisão de se aquilombar pela necessidade básica de existir, a priori, não é uma decisão política para acabar com o sistema

escravista, pois o escravo sequer era sujeito, ao contrário de outros abolicionistas brancos ou negros livres que se articularam para tal. Posteriormente, o movimento de se aquilombar é tomado como ato político e certamente utilizado pelo conjunto de iniciativas que culminou em nossa falsa abolição assinada pela Princesa Isabel, porém...

**“O quilombo (era) uma instituição natural na sociedade escravista. As fugas sucessivas que decorriam da própria situação do escravo, exigiam que se organizassem núcleos capazes de receber o elemento rebelde que necessitava, como é natural, de conviver com semelhantes para sobreviver.”**

Para concluir minha base de argumento sobre soberania e partirmos para a soberania de dados quero deixar demarcado que não existe uma forma exclusiva de se buscar por soberania, afinal como o próprio Clóvis postula em muitas de suas obras, os quilombos são uma forma de soberania, mas existem as guerrilhas, os abolicionistas articulados e até mesmo conexões ditas ilegais para a época que são estratégias utilizadas pelos indígenas e africanos em nosso território em prol de sua soberania e liberdade. O ponto de maior atenção que busquei traçar neste tópico é a visão do que é ser soberano e como que qualquer construção dentro de bases colonizadoras é apenas uma falsa liberdade e manutenção de relações exploratórias, nocivas e mais uma vez de perpetuação colonizadora. Desde que o Brasil foi fundado, qualquer iniciativa de soberania de fato foi construída para a gente, pela gente, no território que a gente escolheu, com nossas regras e costumes e jamais para aqueles que nos colonizaram e insistem em nos manter em determinados espaços. Digo isso pois não há possibilidade de se construir soberania em acordo com quem lhe subjuga.

## **A nossa soberania digital já foi posta à prova e perdemos**

Um grande marco para esse debate de soberania veio com o caso conhecido de documentos vazados pelos [Wikileaks](#), que revelou um esquema realizado pelo governo dos Estados Unidos que vigiavam e monitoravam ilegalmente telefones de cargos do alto escalão político brasileiro, como a presidenta em exercício à época Dilma Rousseff. Uma série de documentos comprovou que a Agência Nacional de Inteligência (?) norte americana havia grampeado vários aparelhos celulares de forma ilegal. O mais interessante é que esta revelação ocorreu justamente quando a então presidenta Dilma estava em viagem aos Estados Unidos articulando acordos econômicos e, o governo brasileiro se posicionou informando que tudo se tratava de fatos antigos e com os Estados Unidos se comprometendo a não repetir a ilegalidade. Vejam, na teoria, o Brasil e os Estados Unidos são soberanos em seus territórios e leis, porém após

uma infração ser comprovada, e termos nosso sigilo e troca de informações criminosamente prejudicada, estabelecemos uma relação de confiança que tudo não iria se repetir.

Esta contradição se torna mais ultrajante quando olhamos para os debates atuais, correntes em 2024 sobre soberania digital (que é o guarda chuva da soberania de dados). Atualmente a União Européia utiliza bastante o conceito de soberania digital que vem influenciando os trabalhos acadêmicos e de Governo e que se baseiam genericamente em três pilares para entender a soberania de dados:

1. Seria a autonomia de segurança e estrutura para garantir a autonomia de sua população de interferências externas?
2. Ou ainda o desenvolvimento econômico nacional? Como é possível fomentar essa agenda em uma economia transnacional?
3. Por fim, surge uma terceira ideia que é a capacidade de autodeterminação digital, garantindo às populações locais os direitos de tomarem decisões sobre os fluxos de seus dados internos.

Apoiados em qualquer uma das três perspectivas, poderíamos concluir, baseado nos acontecimentos do wikileaks que nem o Estado Brasileiro possui soberania digital ou de dados sobre seus fluxos e comunicações! Pois apenas nesta ocasião tivemos nossas comunicações sofrendo total interferência externa, o que pode ter acabado afetando acordos comerciais baseados unilateralmente em informações privilegiadas por parte dos Estados Unidos e que também não tivemos a oportunidade de retaliação ou reparação, apenas de manutenção de acordos e exploração do nosso petróleo. **Por isso, reafirmo que soberania só é possível para gente. Quando a gente faz para gente e só pela gente, que acordos convencionais de soberania são apenas formas de manutenção do poder.**

Numa perspectiva ilusória de soberania, cada país regula e legisla para dentro de suas fronteiras e possui completa autonomia para isso, porém a história e o último exemplo que trouxe já comprovam o contrário. Você não precisa concordar comigo para que eu te prove que isso é apenas uma ilusão. O Brasil, recentemente, foi altamente elogiado por ter elaborado sua própria legislação de proteção de dados (LGPD) em 2018, que garante diversos aspectos que contribuem para uma possível agenda de soberania, inclusive garantindo direitos para tratamento de dados pessoais de brasileiros no exterior. Porém, basta a gente pensar em um exemplo de troca transnacional para entendermos que não há uma soberania garantida. Por exemplo: “como ficam os dados biométricos de uma criança que passa por uma fronteira internacional?”. Em muitos aeroportos mundiais existem máquinas fotográficas que captam o rosto de todas as pessoas estrangeiras que entram naquele país e eventualmente armazenam a imagem da fotografia e a comparam com imagens armazenadas de bancos de imagens de identificação operado por outro país. Ou seja, apesar de que nossa legislação garanta que nossos dados pessoais possuem uma série de restrições

para serem tratados internacionalmente, não há nenhuma opção para quando você, ou uma criança que esteja com você, ao entrar em outro país não tenha seu dado pessoal processado. Eu não estou questionando sobre os motivos ou consequências, mas simplesmente te mostrando um ponto de vista que a ideia que temos sido ensinado de soberania não corresponde à práticas soberanas principalmente entre países com distintas posições econômicas.

Estudos mais progressistas sobre soberania digital e de dados têm defendido a perspectiva da terceira abordagem que citei, da auto afirmação. Onde os indivíduos ou cidadãos de um país têm o direito de se autoafirmar e decidirem sobre seus dados e direitos em busca de uma agenda soberana. É nessa perspectiva que muitos regimes democráticos têm realizado tomada de subsídios, consultas públicas e planejamentos participativos na busca de mitigar a exclusão de processos que apenas reforçam a marginalização de alguns grupos. Porém, como mostramos anteriormente, não temos necessariamente um cenário de inclusão que possibilite que tais processos garantam uma participação efetiva e muito menos a defesa de seus interesses em cenários e ambientes ditos formais.

## E se insistíssemos em manter uma discussão jurídica e econômica?

A despeito dos aspectos históricos que já apresentei neste capítulo, se precisássemos traçar uma análise seccional apenas do atual aparato jurídico econômico sobre soberania digital e de dados eu concordaria com o [artigo](#) publicado pela advogada Flavia Leffevre que defende que nacionalmente temos uma estrutura legal robusta que garante uma maior soberania nacional. Em seu texto, Flávia explica sobre as implicações da soberania digital, focando nos desafios legais e políticos enfrentados pelos países na era digital. Ela ainda aborda questões como a proteção de dados, a influência das grandes corporações tecnológicas, e a importância de políticas públicas que garantam a autonomia digital dos estados. Ela enfatiza a necessidade de uma governança digital que respeite os direitos dos cidadãos e promova a inclusão digital. Sobre a proteção de dados em si, o texto aborda a importância de proteger os dados pessoais dos cidadãos em uma perspectiva local e em seu texto fica explícito o desafio de que as propostas apresentadas para proteção de dados são inviáveis e insuficientes frente ao rápido avanço tecnológico e às ameaças cibernéticas. Além disso, a influência das corporações tecnológicas têm tornado o debate legislativo, não só no Brasil, impossível de ser feito de forma autônoma, considerando o contexto global e as interdependências econômicas. **Por fim, como garantir que os cidadãos se auto afirmem e lutem por seus direitos se ainda não alcançamos uma cenário onde a nossa população entenda ou esteja incluída nos debates digitais?**

Por isso, que trabalhos como o de [Shoshana Zuboff](#) são tão fundamentais, ao comprovarem que em uma ambiente capitalista não é possível traçar uma agenda soberana, pois como que um país pode legislar de forma autônoma e

soberana em um contexto onde empresas como as do GAFAM (Google, Apple, Facebook, Amazon e Microsoft) possuem faturamentos superiores aos de muitos estados? Segundo Shoshana Zuboff, a ausência de soberania em uma sociedade capitalista é agravada pelo poder dessas corporações sobre os dados e a vigilância. Dessa forma, não temos como implementar leis rigorosas sobre privacidade e proteção de dados, ou assegurar que essas corporações paguem impostos justos nos países onde operam. E este processo é justamente o que levou o Brasil a parar de investir em infraestrutura tecnológica e promover empresas locais que aumentaram sua dependência das gigantes empresas estrangeiras.

## **Agora pega tua merenda - visões periféricas sobre soberania de dados**

É por isso, que não apenas eu, mas muitos ativistas brasileiros têm defendido uma agenda de soberania de dados baseada na visão quilombola de sobrevivência. O atual jogo tecnológico nos deixou dependente de forma generalizada das maiores empresas do ramo da tecnologia que armazenam nossos dados, intermediam nossos processos e fluxo de dados e em grande medida tem até mesmo financiado nossas atividades em torno de uma possível soberania. Sabendo que não temos como depor o imperialismo tecnológico, decidimos fundar os nossos próprios territórios online, com nossas regras e culturas que respeitem nossos interesses em prol do nosso progresso, um quilombo cibernético.

Uma dessas iniciativas foi construída baseada na metodologia da Geração Cidadã de Dados (GCD) que é um conjunto de ações que permitem aos próprios cidadãos coletarem, armazenarem e analisarem seus próprios dados. Essas ações nem sempre ocorrem fora do domínio das empresas que compõem o GAFAM, mas desafiam a lógica de apropriação deliberada defendida por elas. Sendo assim, organizações e coletivos têm aprendido e construindo suas próprias metodologias de coleta de dados, armazenando seus dados em nuvens próprias ou ainda com criptografia própria em servidores proprietários para ter sua independência dentro do império em que somos explorados.

Uma dessas iniciativas é o Contrate Quem Luta, que é um exemplo de soberania de dados dentro de uma economia capitalista e neoliberal. A plataforma utiliza recursos proprietários para desenvolver ferramentas que contemplem a liberdade e inovação da periferia, onde profissionais do Movimento Sem Teto podem se cadastrar e estipular seus valores para serviços necessários a quem se interessar, fazendo com que esses profissionais não precisem depender de plataformas digitais que acabam se beneficiando financeiramente apenas por intermediar a contratação. Bem como os projetos de GCD que têm sido desenvolvidos pela sociedade civil brasileira, não temos tempo e recurso disponíveis para criar tudo de forma independente literalmente, mas assim como os quilombos que existiam dentro de um império colonizador, criamos, ditamos e nos protegemos para exercermos o que nós mesmos queremos exercer de liberdade.

Um outro projeto de GCD que estimula a agenda de soberania de dados é o projeto criado pelo data\_labe para combater irregularidades de saneamento básico na

favela da Maré, chamado **cocozap**. Nesse projeto, a organização desenvolveu uma engenharia de serviço que apesar de depender do início da conversa via whatsapp, todo o processo obedece fluxos de análise e proteção de dados que visam proteger o morador que denuncia as irregularidades e análise de forma transparente e aberta as denúncias recebidas para encaminhar de forma organizada e estruturada as demandas de saneamento da comunidade às autoridades públicas responsáveis. Em sua **metodologia**, o data\_labe explica quais ferramentas elaborou de criptografia e hashing que garantem a segurança de dados do morador, tornando impossível o uso dos dados pessoais para outros fins. Para isso ter se tornado possível, a equipe inteira do data\_labe teve que aprender sobre proteção e segurança de dados a fim de desenvolverem juntos rotinas que de fato protegessem os dados pessoais envolvidos no projeto. Ou seja, a equipe de dados e tecnologia sozinha jamais teria conseguido colocar em prática uma rotina segura, bem como a consultoria jurídica em ação na organização não teria conseguido implementar políticas de proteção de dados que fizessem sentido para o trabalho na periferia.

O que quero dizer com esse ponto é que não há uma única forma de garantir soberania de dados, existem muitas. **Pois fundamentalmente, o que garante a soberania e proteção de dados das pessoas envolvidas é o respeito e entendimento da potência de cada grupo envolvido no processo e, assim, cada grupo entenderá e desenvolverá seus protocolos.** Para isso, é necessário compreender os mecanismos que nos vulnerabilizam para entender como aquilombar os processos que nos fazem bem. Vejam, não estou aqui defendendo um descumprimento da nossa LGPD ou demais aparatos jurídicos em vigor, mas entender que esses mecanismos não nos contemplam e eventualmente nos vulnerabilizam. A partir daí como garantir um cuidado que faça sentido pra gente, onde possamos existir com nossa plenitude?

Te darei um exemplo que pode parecer abstrato, mas tem sido cada vez mais real e repetido até mesmo dentro das organizações da sociedade civil. Em processos de seleção ou inscrição de eventos tem sido cada vez mais comuns a disponibilização de formulários online para que a pessoa interessada coloque seus dados pessoais para a inscrição, porém cientes de que muitos desses formulários são hospedados em plataformas estrangeiras, algumas organizações tem limitado suas perguntas a apenas perguntas essenciais para cumprimento da finalidade da inscrição, ou seja, mesmo cientes que para a “execução do contrato” poderíamos solicitar variáveis como gênero e raça/cor, estamos cientes de que essas informações são utilizadas para realizarem perfilamento profundo do usuário e venda de dados pessoais para terceiro para fins de publicidade. **Ou seja, conscientes de que não temos nada a ganhar obedecendo às tendências e normas vigentes no campo tecnológico, fundamos novas práticas que possam de fato garantir a segurança dos nossos usuários.**

Notem, que o trabalho de GCD poderia ainda não garantir ou contribuir para uma soberania de dados, se decidisse coletar dados massivos e simplesmente entregá-los aos servidores internacionais dos quais muitas de nossas organizações dependem. Porém, seguindo a lógica de processos para benefício



próprio, organizações têm reduzido perguntas invasivas e não fundamentais para realização da atividade e adicionado camadas de segurança da informação para não entregarem dados coletados em suas ações de incidência de graça nas mãos de grandes oligopólios, mesmo dependendo de suas estruturas digitais para funcionarem.

Eu tenho ainda outros projetos a mencionar, que utilizam a GCD ou não, que se preocupam com a soberania de dados dos seus usuários como o [PretaLab](#), gerido pelo Olabi que não negocia o compartilhamento dos dados pessoais de suas alunas e apoiadas a nenhum financiador ou terceiro. Além disso suas análises de perfil e de impacto são feitas de forma local e não compartilhada. Outra organização de longa data que tem a soberania de dados como um pilar de suas ações é o Coletivo [Intervozes](#), que ao coletar dados pessoais utiliza plataformas de software livre e aberto, desenvolvidas em território nacional com extrema atenção às políticas de privacidade de seus apoiados. Destaco ainda as iniciativas do [Observatório do Marajó](#), que atuando em uma região de extrema escassez de tecnologia tem se voltado a desenvolver mapeamentos e coletas analógicas para garantir a segurança dos habitantes da Ilha do Marajó e não entregarem dados nas mãos das empresas de tecnologia ou sob risco de eventuais perseguidores dos defensores territoriais e de direitos humanos da região.

Obviamente que existem outras organizações que entendem e se preocupam com a segurança dos dados pessoais que coletam, porém estes projetos centralizam suas ações e planejamentos a partir da garantia de que os dados coletados, armazenados e processados **atendam aos interesses dos proprietários** daqueles dados. Estabelecendo suas rotinas, suas análises e seus armazenamentos. Sendo assim, continuo defendendo que a soberania está pautada na possibilidade de se rebelar. Seja a priori, quando se retira das mãos das grandes empresas ou Estado, qualquer autonomia sobre os dados envolvidos nas ações, ou garantindo que a continuação de seus processos e metodologias dependerão apenas de sua própria vontade e beneficiados. Vejam que não cito um teórico, uma pesquisa, ou uma fonte para referência na minha conclusão, o fiz no decorrer do texto. Pois assim como nossos antepassados sabiam, a liberdade sempre está dentro de nós e para alcançarmos basta nos unirmos e decidirmos o que é melhor pra gente, mesmo que seja debaixo dos olhos daqueles que nos aprisionam ou usurpam dos nossos direitos. Soberania é fazer coletivo para benefício próprio.



**Conclusão**

**DESENHANDO  
O FUTURO:  
UM MARCO  
PARA A GCD**

**Bruno Sousa**



## BRUNO SOUSA

Co-fundador do Instituto Decodifica, atua como coordenador de comunicação; co-fundador da Agência Metáfora, onde atua como Diretor Executivo e de Criação. Jornalista com foco em raça, segurança pública, direitos humanos e tecnologia. Com passagem pelas redações do The Intercept Brasil e Agência Narra, também colabora para veículos como UOL, Estadão, Meia Hora, Folha de São Paulo, Vice e Huffpost. Atuou na comunicação e pesquisa no CESeC pelo projeto Panóptico, na comunicação institucional da Redes da Maré e como coordenador de marketing na Barkus Educacional.

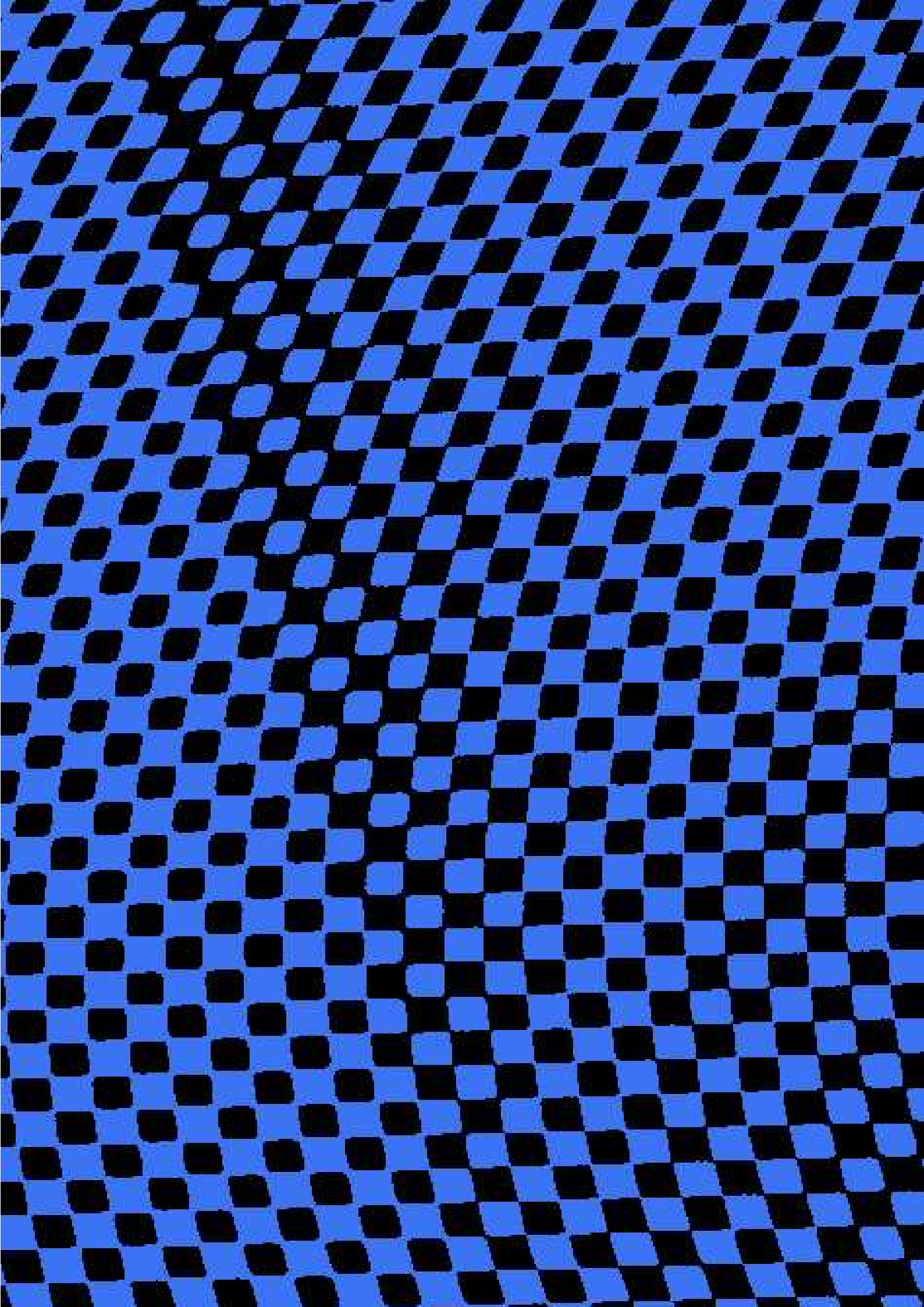
O livro que ora se encerra nos conduziu por uma jornada crucial: a intersecção entre dados, justiça racial e a construção de um futuro mais equitativo para as periferias. Ao explorar a Geração Cidadã de Dados (GCD) e sua relação com a Lei Geral de Proteção de Dados (LGPD), este trabalho oferece uma contribuição inédita para o campo da pesquisa e da prática.

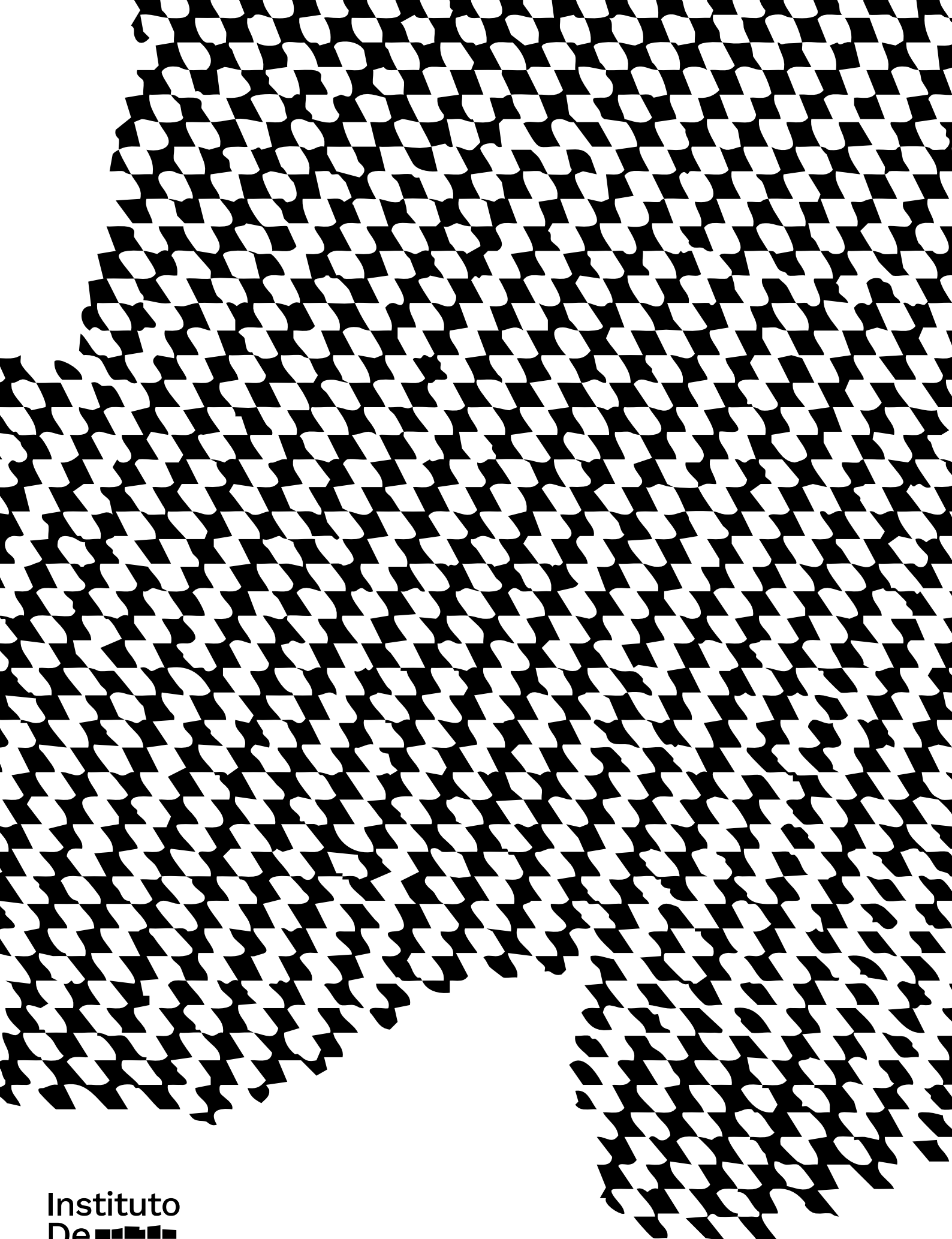
Ao longo das páginas, demonstramos como a GCD, quando realizada de forma ética e responsável, pode ser uma ferramenta poderosa para amplificar as vozes marginalizadas e influenciar a formulação de políticas públicas mais justas. No entanto, também destacamos os desafios e riscos associados ao uso de dados, especialmente no contexto das desigualdades sociais e raciais.

A proteção de dados, nesse contexto, não é um mero detalhe técnico, mas um direito fundamental que se entrelaça com a luta por justiça social. A LGPD surge como um marco legal fundamental para garantir a privacidade dos indivíduos e a utilização ética dos dados. Este livro oferece um guia prático para que instituições do Terceiro Setor e organizações que utilizam a GCD possam se adequar a esta legislação e garantir a proteção dos dados das comunidades que atendem.

Ao trazer à tona a importância da soberania de dados e a necessidade de construir um futuro digital mais justo e democrático, este trabalho se coloca como um marco para o debate sobre a justiça de dados no Brasil. Acreditamos que as ideias aqui apresentadas podem inspirar pesquisadores, ativistas, policymakers e a sociedade civil, como um todo, a se engajarem nessa luta, buscando soluções inovadoras e criativas para os desafios do século XXI.

Este livro é mais do que um simples estudo; é um chamado à ação. Ao oferecer um arcabouço teórico e prático para a implementação da LGPD no contexto da GCD, contribuímos para fortalecer a atuação de instituições do Terceiro Setor em um contexto no qual possam ainda robustecer uma cultura de proteção de dados e garantir que estes sejam utilizados de forma ética e responsável em prol da construção de uma sociedade mais justa e equitativa.





Instituto  
De   
codifica

